Final Review Draft October 31, 2007 - Cisco Confidential

Cisco 12000 Series Router Configuration Guide for Cisco IOS Release 12.0S

Cisco IOS Release 12.0S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number:

Cisco 12000 Series Router Configuration Guide for Cisco IOS Release 12.0S

CONTENTS

Final Review Draft October 31, 2007 - Cisco Confidential

CHAPTER 1

Cisco 12000 Series Internet Router Basics

Feature History

Release	Modification
11.2GS	The Cisco 12008 and Cisco 12012 Internet Routers were introduced.
12.0(8)S	The Cisco 12016 Internet Router was introduced.
12.0(15)S	The Cisco 12416 Internet Router was introduced.
12.0(16)S	The Cisco 12410 Internet Router was introduced.
12.0(17)S	The Cisco 12406 Internet Router was introduced.
12.0(21)S	The Cisco 12404 Internet Router was introduced.

The Cisco 12000 Series Internet Routers include a number of platforms and comprise a wealth of features that have been introduced since the product was released. This document describes how to configure and troubleshoot the Cisco 12000 Series Internet Routers on a system level. It does not describe hardware installation procedures, nor does it describe protocol and routing configurations.

Feature Overview

The Cisco 12000 Series Internet Routers are a class of routers that perform Internet routing and switching at up to gigabit speeds. Meeting the exponential growth in demand for Internet bandwidth, these routers bring scalability and high-performance carrier-class services to IP-based networks.

Benefits

The Cisco 12000 Series Internet Routers offer a wide range of benefits, including:

- High-end routing for service provider backbone and edge applications, enabling service providers to meet the challenge of building packet networks to satisfy services demand while increasing profitability
- Up to 10 Gbps per slot systems
- Wide range of interfaces, including Packet over SONET (POS), Asynchronous Transfer Mode (ATM), Dynamic Packet Transport/Resilient Packet Ring (DPT/RPR), and Gigabit Ethernet (GbE)
- Reliability
- Rich set of service enablers

- Low cost of ownership
- Proven investment protection, including systems that can be upgraded in the field to increase switching capacity
- IP and MPLS networks

Supported Platforms

Table 1-1 details the platforms included in the Cisco 12000 Series, the number of slots and capacity of each platform, and supported Cisco IOS releases.

Table 1-1 Cisco 12000 Series Internet Router Platforms

Platform	Rack Size	Number of Slots	Switch Fabric Capacity	Number of Line Card Slots[1]	Number of Switch Fabric Slots
Cisco 12008	1/3	8	40 Gbps	7	3 SFC[2], 2 CSC[3]
Cisco 12012	Full	12	60 Gbps	11	3 SFC, 2 CSC
Cisco 12016	Full	16	80 Gbps[4]	15	3 SFC, 2 CSC
Cisco 12404	1/8	4	80 Gbps	3	1 board[5]
Cisco 12406	1/4	6	120 Gbps	5	3 SFC, 2 CSC
Cisco 12410	1/2	10	200 Gbps	9	5 SFC, 2 CSC
Cisco 12416	Full	16	320 Gbps	15	3 SFC, 2 CSC

[1] One slot is used by the route processor card (RP). If two RPs are present for redundancy purposes, there is one less slot available for line cards.

[2] Switch fabric card

[3] Clock scheduler card

[4] The Cisco 12016 Internet Router can be upgraded to a Cisco 12416 Internet Router using a switch fabric upgrade kit.

[5] The Cisco 12404 Internet Router contains a single board that performs the functionality of 3 SFCs and 1 CSC.

Supported Line Cards

Cisco 12000 Series Internet Routers offer an extensive portfolio of line cards, including Packet over SONET (POS), channelized and digital signal, Asynchronous Transfer Mode (ATM), Ethernet, and Dynamic Packet Transport (DPT). These line cards deliver high performance, guaranteed priority packet delivery, and service-transparent online insertion and removal (OIR).

Each of these line cards is distinguished by its underlying engine type. Cisco 12000 Series Internet Router line cards are designed to support high-speed packet forwarding performance in the core of an IP network. Engine 3 and Engine 4+ line cards are designed for edge applications and implement enhanced IP services (such as QoS) in hardware with no performance impact.

Available line cards for the Cisco 12000 Series Internet Routers as of November 2002 are listed in Table 1-2 through Table 1-7.

Table 1-2 POS/SDH Line Cards

Line Card	Engine	Chassis Supported	First Cisco IOS Release
4-Port OC-3c/STM-1c POS/SDH	0	All	12.0(5)S
1-Port OC-12c/STM-4c POS/SDH	0	All	12.0(10)S
1-Port OC-48c/STM-16c POS/SDH	2	All	12.0(10)S
4-Port OC-12c/STM-4c POS/SDH	2	All	12.0(10)S
8-Port OC-3c/STM-1c POS/SDH	2	All	12.0(10)S
16-Port OC-3c/STM-1c POS/SDH	2	All	12.0(10)S
16-Port OC-3c/STM-1c POS/SDH	3 ISE	All	12.0(21)S
4-Port OC-12c/STM-4c POS/SDH	3 ISE	All	12.0(21)S
1-Port OC-48c/STM-16c POS/SDH	3 ISE	All	12.0(21)S
4 and 8-Port OC-3c/STM-1c POS/SDH	3 ISE	All	12.0(22)S
4-Port OC-48c/STM-16c POS/SDH	4+	124xx	12.0(15)S
1-Port OC-192c/STM-64c POS/SDH	4/4+	124xx	12.0(15)S

Table 1-3 ATM Line Cards

Line Card	Engine	Chassis Supported	First IOS Release
4-Port OC-3c/STM-1c ATM	0	All	12.0(5)S
1-Port OC-12c/STM-4c ATM	0	All	12.0(7)S
4-Port OC-12c/STM-4c ATM	2	All	12.0(13)S
8-Port OC-3c/STM-1c ATM	2	All	12.0(22)S
4-Port OC-12c/STM-4c ATM ISE	3	All	12.0(25)S

Table 1-4 Ethernet Line Cards

Line Card	Engine	Chassis Supported	First IOS Release
8-Port Fast Ethernet	1	All	12.0(10)S
1-Port Gigabit Ethernet	1	All	12.0(10)S
3-Port Gigabit Ethernet	2	All	12.0(11)S
10-Port 1-Gigabit Ethernet	4	124xx	12.0(22)S
1-Port 10-Gigabit Ethernet	4	124xx	12.0(23)S
10-Port Modular Gigabit Ethernet	4	124xx	12.0(23)S
4-Port Gigabit Ethernet ISE	3	All	12.0(25)S

Table 1-5 Dynamic Packet Transport (DPT) Line Cards

Line Card	Engine	Chassis Supported	First IOS Release
2-Port OC-12c/STM-4c DPT	1	All	12.0(10)S
1-Port OC-48c/STM-16c DPT	2	All	12.0(15)S
4-Port OC-48c/STM-16c DPT	4+	124xx	12.0(23)S
1-Port OC-192c/STM-64c DPT	4+	124xx	12.0(23)S
4-Port OC-12c/STM-4c DPT ISE	3	All	12.0(24)S

Table 1-6 Channelized Line Cards

Line Card	Engine	Chassis Supported	First IOS Release
2-Port Channelized OC-3c/STM-1c to E1/T1	0	All	12.0(17)S
1-Port Channelized OC-12c/STM-4c to DS3	0	All	12.0(5)S
1-Port Channelized OC-12c/STM-4c to OC-3c/STM-1c	0	All	12.0(5)S
6-Port Channelized T3 (T1)	0	All	12.0(14)S
4-Port Channelized OC-12c/STM-4c (DS3/E3, OC-3c/STM-1c) POS/SDH	3 ISE	All	12.0(21)S
1-Port Channelized OC-48c/STM-16c (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH	3 ISE	All	12.0(21)S

Table 1-7 Electrical Interface Line Cards

Line Card	Engine	Chassis Supported	First IOS Release
6-Port DS3	0	All	12.0(10)S
12-Port DS3	0	All	12.0(10)S
6-Port E3	0	All	12.0(15)S
12-Port E3	0	All	12.0(15)S

Related Documents

For more information concerning the Cisco 12000 Series Internet Router hardware, refer to the installation and configuration guide for the specific platform, as listed following:

- *Cisco 12008 Internet Router Installation and Configuration Guide*
- *Cisco 12012 Internet Router Installation and Configuration Guide*
- *Cisco 12016 Internet Router Installation and Configuration Guide*
- *Cisco 12404 Internet Router Installation and Configuration Guide*

- *Cisco 12406 Internet Router Installation and Configuration Guide*
- *Cisco 12410 Internet Router Installation and Configuration Guide*
- *Cisco 12416 Internet Router Installation and Configuration Guide*

For more information concerning specific line cards and their configuration, refer to the line card installation and configuration notes located at http://www.cisco.com/univercd/cc/td/doc/product/core/cis12000/linecard/index.htm.

Supported MIBs and RFCs

MIBs

The following Management Information Bases (MIBs) apply:

- APS MIB
- ATM MIB
- ATM Forum MIB
- BGP4 MIB
- Cisco AAL5 MIB
- Cisco ATM Ext MIB
- Cisco Bulk File MIB
- Cisco Car MIB
- Cisco CDP MIB
- Cisco Config Copy MIB
- Cisco Config MAN MIB
- Cisco Enhanced WRED MIB
- Cisco Entity FRU Control MIB trap support
- Cisco Environmental MIB
- Cisco Frame Relay MIB
- Cisco Flash MIB
- Cisco FTP Client MIB
- Cisco IETF-ATM2-PVCTRAP-MIB
- Cisco IMAGE MIB
- Cisco IP Stat MIB
- Cisco IPMROUTE MIB
- Cisco Memory Pool MIB
- Cisco Ping MIB
- Cisco Process MIB
- Cisco Queue MIB
- Cisco RTTMON MIB
- Cisco Syslog MIB

- Cisco TCP MIB
- Cisco VLAN IFTABLE Relationship MIB
- Community MIB
- Expression MIB
- If MIB
- IGMP MIB
- Int Serv Guaranteed MIB
- Int Serv MIB
- IP MROUTE MIB
- IPv6 MIB
- Notification Log MIB
- MQC MIB (Engines 2, 3, 4, and 4+)
- Old Cisco Chassis MIB
- Old Cisco CPU MIB
- Old Cisco Interfaces MIB
- Old Cisco IP MIB
- Old Cisco Memory MIB
- Old Cisco System MIB
- Old Cisco TCP MIB
- Old Cisco TS MIB
- Optical MIB
- PFE MIB
- PIM MIB
- RMON MIB
- RS-232 MIB
- RSVP MIB
- SNMPv2 MIB
- TCP MIB
- UDP MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator, found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

The following Requests for Comments (RFCs) apply:

- RFC 1213
- RFC 1253
- RFC 1315
- RFC 1398
- RFC 1407
- RFC 1595—For RFC 1595, the Cisco 12000 Series Internet Router does not support SONET Far End Line Group, SONET Far End Path Group, SONET VT Group, and SONET Far End VT Group.

CHAPTER 2

Basic Configuration of the Cisco 12000 Series Internet Router

This chapter describes how to boot and configure the Cisco 12000 Series Internet Router. It discusses the following subjects:

- Cisco IOS Software Images, page 2-1
- Configuring the Router, page 2-3
- Configuration Tasks, page 2-5
- Route Processing, page 2-9
- PCMCIA Flash Memory Tasks, page 2-11
- Upgrading and Backing Up Cisco IOS Software Images and Configuration Files, page 2-13

For information on installing your router or LED indications during the boot process, refer to your installation and configuration guide.

Cisco IOS Software Images

By default, your router ships with a Cisco IOS software image preloaded into the Flash memory card or Flash disk inserted in PCMCIA slot 0 on the Route Processor (RP). Initially, your router is configured to boot from this image. You can change this default and configure the router to boot from a Flash memory card or Flash disk in slot 1 on the RP, or from a TFTP server. If you specify that the router boot from an image on a TFTP server, you must verify that you have an Ethernet connection to the URL of the TFTP server.

In addition, there is a mini-software image preloaded into the single inline memory module (SIMM) or bootflash. This image can be used to boot the router if there is no other valid image available. It provides a limited number of configuration commands that you can use to locate a valid Cisco IOS software image or correct basic configuration problems. This image provides no routing capabilities.

Related issues are discussed in the following sections:

- Locating a Valid Cisco IOS Software Image, page 2-2
- Manually Booting from a Cisco IOS Software Image, page 2-2

Locating a Valid Cisco IOS Software Image

If your router does not find a valid system software image, the system should enter read-only memory (ROM) monitor mode and display the ROM monitor prompt (`Rommon>`). From this mode, you can use the following commands to locate a valid system image.

Command	Purpose
`Rommon 1>` **`dir bootflash:`**	Displays the contents of the single inline memory module (SIMM), also known as the bootflash, on the route processor (RP). Images in the bootflash are mini-software images that are used for basic configuration tasks only.

`Rommon 2>` **`dir slot0:`**
`or`
`Rommon 2>` **`dir slot1:`**
	Displays the contents of the Flash memory card (if present) in either PCMCIA slot 0 or slot 1.

`Rommon 3>` **`dir disk0:`**
`or`
`Rommon 3>` **`dir disk1:`**
	Displays the contents of the Flash memory disk (if present) in slot 0 or slot 1.

The following examples show the output from these commands:

```
Rommon 1> dir bootflash:
Directory of bootflash:/

    1  -rw-     5043356   Jan 01 2000 00:01:15  gsr-boot-mz.120-8.S
Rommon 2> dir slot0:
Directory of slot0:/

    1  -rw-    13778192   Jan 14 2002 18:24:26  gsr-p-mz.120-19.S.bin
   12  -rw-        3973   Sep 03 2002 23:09:47  ozRun

20578304 bytes total (6762344 bytes free)
```

Manually Booting from a Cisco IOS Software Image

If your router does not find a valid system software image, you will need to boot an image manually by issuing the appropriate ROM monitor mode **boot** command. Once you have located a software image, use one of the following forms of the **boot** command to boot the router:

Command	Purpose
`Rommon 3>` **`boot`**	(No argument.) Boots the default image found in the SIMM or bootflash. This image is preloaded into the SIMM at the factory.
`Rommon 3>` **`boot flash`**	(Does not specify a particular PCMCIA slot.) Attempts to boot the router using the first file found in the Flash memory card inserted in slot 0 of the RP.
`Rommon 3>` **`boot slot0:`** *`filename`*	Boots the router using the specified file on the Flash memory card in slot 0 of the RP.
`Rommon 3>` **`boot disk0:`** *`filename`*	Boots the router using the specified file on the Flash memory disk in slot 0 of the RP.
`Rommon 3>` **`boot slot1:`** *`filename`*	Boots the router using the specified file on the Flash memory card in slot 1 of the RP.

Command	Purpose
`Rommon 3> boot disk1: filename`	Boots the router using the specified file on the Flash memory disk in slot 1 of the RP.
`Rommon 3> boot bootflash: filename`	Boots the router using the specified file on the SIMM (bootflash) on the RP.
`Rommon 3> boot tftp: filename [host]`	Boots the router using the specified file on a host TFTP server in the network.

If you did not change the contents of the software configuration register, the factory default setting of 0x0102 in the software configuration register causes the system to boot from the Cisco IOS software image on a Flash memory card or Flash disk inserted in PCMCIA slot 0 the next time you boot the router.

Configuring the Router

You can perform a basic configuration for your router by using either of the following methods:

- Setup facility or the **setup** command.
  This method provides an interactive script to guide you through the configuration process. It is described in the "Configuring the Router Using the Setup Command" section on page 2-3.
- Global configuration mode through the Cisco IOS command line user interface.
  This method requires you to enter configuration commands on a line-by-line basis at the console, without being prompted by a configuration script. It is described in the "Using Global Configuration Mode" section on page 2-4.

You can use whichever method suits your operating style and your knowledge of network configuration requirements.

Whether you choose to use the **setup** command facility or the global configuration mode to configure the router to operate in your networking environment, be sure you know the following before starting the configuration procedure:

- Interfaces on the router
- Protocols the router is routing
- Network addressing scheme for the router
- Password scheme for your environment

Note Before you can configure the router, a console terminal should be connected to the console port on the faceplate of the RP. For more information on router installation and boot procedure, refer to your installation and configuration guide.

Configuring the Router Using the Setup Command

One method of configuring the router is to use the **setup** command, also known as the **setup** command facility. During the first startup of an unconfigured router, the system automatically starts the **setup** command facility, which enables you to begin configuring your router. The **setup** command facility presents a structured, interactive script that guides you through the configuration process with prompts for global (system-wide) parameters and interface (line card) parameters.

You can also invoke the **setup** command facility at any time by issuing the **setup** command at the privileged EXEC mode prompt (`Router#`), which invokes the same configuration script that appears automatically during the first startup of an unconfigured router. You can use the **setup** command to alter previously entered configuration information or to enter a new configuration. The advantage of using the **setup** command facility is that the system uses an interactive script to guide you through the configuration process.

If you use the **setup** command facility to alter the router configuration, you must allow the entire **setup** command facility script to run, until you come to the item that you want to change. To accept default settings for items that you do not want to change, press the console keyboard **Return** key. To return to the privileged EXEC prompt without making changes, press **Ctrl-C**. To access help text in the setup command facility, press the question mark key (?) at any prompt.

When you complete your changes, the **setup** command facility displays the configuration command script that was created as a result of the changes you entered during the setup session. It also queries if you want to use this configuration. If you answer Yes, the configuration is saved to NVRAM. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

Following is an example of the initial output from the **setup** command facility session:

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: Yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic setup only configures enough connectivity
for management of the system, extended setup will ask you
to configure each interface of the system.
```

Note The only observable difference between the configuration script displayed when the **setup** command facility starts automatically on startup, and the script displayed when you manually enter the **setup** command, is that when you enter the command manually, the script displays any previously entered system configuration defaults within square brackets ([ ]).

Using Global Configuration Mode

If you prefer not to use the interactive script of the setup facility, you can manually configure your router using global configuration mode. Global configuration mode enables you to enter configuration commands line by line from the console terminal.

Before you can configure your router using the global configuration mode, you will need to be familiar with the Cisco IOS software command line interface. If you are unfamiliar with the Cisco IOS command line interface, you should read the "Using the Command Line Interface" chapter in the *Configuration Fundamentals Configuration Guide*. That chapter discusses the different command modes, context-sensitive help, and editing features.

To configure your router using global configuration mode, follow these steps:

	Command	Purpose

Step 1	`Continue with configuration dialog?`
	`[yes/no]:` **`no`**
		Enters user EXEC mode on the router without entering the **setup** command facility. You receive this prompt when you initially boot the router. If you have completed the **setup** command facility, you will already be in user EXEC mode and can continue with Step 2.

Step 2	`Router>` **`enable`**
	`Router#`
		Enters privileged EXEC mode on the router. Depending on the system and the software version, you may be prompted for a password. The prompt changes to `Router#` in privileged EXEC mode.

Step 3	`Router#` **`configure terminal`**
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#`
		Enters global configuration mode, from which you can enter most of the configuration commands needed to change the system configuration. The prompt changes to `Router(config)#` in global configuration mode. When you are finished entering configuration commands, press **Ctrl-Z** to exit global configuration mode.

Step 4	`Router(config)#` **`interface`** *`type slot/port`*
	`Router(config-f)#`
		Enters interface configuration mode for the specified interface. In interface configuration mode, you can enter commands to change the interface configuration. The prompt changes to `Router(config-f)#` in interface configuration mode. When you are finished entering configuration commands, press **Ctrl-Z** to exit the configuration mode and return to privileged EXEC mode. Use the **exit** command to return to global configuration mode.

Step 5	`Router#` **`copy running-config startup-config`**
	`or`
	`Router#` **`write memory`**
		Saves the running configuration changes to NVRAM. If you do not save the running configuration to NVRAM, your configuration settings will be lost the next time you reload the router.

In global configuration mode, you will enter all the necessary commands to configure your router. The remainder of this document describes typical configuration tasks that you may need to perform. To display a list of the configuration commands available to you, enter a question mark (**?**) at the prompt or press the designated **help** key on the terminal keyboard while in configuration mode. For more information concerning Cisco IOS configuration commands, refer to the Cisco IOS Command Reference located at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/rbkixol.htm

Configuration Tasks

This section details initializing configuration tasks that should be performed on your router. Each task can be performed using either the setup command facility or the global configuration mode.

- Configuring the Router Host Name, page 2-6
- Configuring Passwords on the Router, page 2-6
- Configuring Ethernet Access for Network Management, page 2-7
- Configuring Line Card Interfaces, page 2-8

Configuring the Router Host Name

The default host name for all routers is “router”. You can change the host name by using the **setup** command or the **hostname** command.

Command	Purpose
`Router>` **`hostname`** *`name`*	Assigns a host name to the router.

When the **setup** command is used, you are prompted to enter a host name, as in the following example:

```
Would you like to enter basic management setup? [yes/no]: Yes
Configuring global parameters:
  Enter host name [Router]: Filo
```

The name you assign the router must follow the rules for ARPANET host names. It must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The name must consist of 63 or fewer characters. For more information, refer to *Requests For Comments (RFC) 1035, Domain Names—Implementation and Specifications*.

Upper- and lowercase characters look the same to many Internet software applications; therefore for ease of use, computer names should appear in all lowercase. For more information, refer to *RFC 1178, Choosing a Name for Your Computer.*

Configuring Passwords on the Router

The commands available at the user EXEC level are a subset of those available at the privileged EXEC level. Many privileged EXEC commands are used to set system parameters, so you should password-protect these commands to prevent their unauthorized use. Following is a subset of the password protection commands, which are accessed via global configuration mode.

Command	Purpose
`Router(config)#` **`enable password`** *`password`*	Configures authentication to access the privileged EXEC commands. After using this command, when you use the **enable** command to enter privileged EXEC mode, you will be prompted for the enable password.
`Router(config)#` **`enable secret`** *`password`*	Configures authentication to access the privileged EXEC commands. The **enable secret** offers better security than the **enable password** because the **enable secret** password is stored using a nonreversible cryptographic function.

`Router(config)#` **`line vty 0 4`**
`Router(config-line)#` **`login`**
`Router(config-line)#` **`password`** *`password`*
	Configures authentication to access a router via incoming Telnet sessions.

`Router(config)#` **`line console 0`**
`Router(config-line)#` **`login`**
`Router(config-line)#` **`password`** *`password`*
	Configures authentication to access the console terminal.

Password protection can also be configured using the **setup** command facility, as in the following example:

```
  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
```

```
Enter enable secret [<Use current secret>]: esecret

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: epassword

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: tpassword
```

For maximum security, the **enable secret** and the **enable password** should be different. If you use the same password for both the **enable secret** and **enable password** prompts during the **setup** process, the system accepts it but issues a warning indicating that you should enter a different password.

An **enable secret** can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an **enable password** can contain any number of uppercase and lowercase alphanumeric characters. You cannot use a number as the first character. Spaces, however, are valid password characters. For example, `two words` is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Make a note of all passwords you set and store that information in a secure location for future reference.

For more detailed information on how to establish password protection or configure privilege levels, refer to the *Security Configuration Guide*, located at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/index.htm

Configuring Ethernet Access for Network Management

You can configure Ethernet connectivity to your router via the route processor (RP) for network management purposes. The RJ-45 and MII receptacles on the faceplate of the GRP and the RJ-45 receptacles on the faceplate of the PRP are IEEE 802.3u-compliant interfaces. You can use one interface or the other, but not both at the same time.

To configure Ethernet connectivity, perform the following procedure. The IP address and subnet mask are examples only. You will need to obtain this information from your network administrator.

	Command	Purpose
Step 1	`Router(config)# interface ethernet 0`	Enters interface configuration mode on the Ethernet interface.
Step 2	`Router(config-if)# ip address 10.10.1.1 255.255.0.0`	Specifies the IP address and subnet mask for the interface.

Ethernet connectivity can also be configured using the **setup** command facility, as in the following example:

```
Configuring interface Ethernet0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
    IP address for this interface: 10.10.1.1
    Number of bits in subnet field: 8
    Class A network is 10.0.0.0, 8 subnet bits; mask is 255.255.0.0
  Configure CLNS on this interface?: yes
```

Configuring Line Card Interfaces

Because of the wide variety of line cards supported by the Cisco 12000 Series Internet Router, you should refer to the configuration note that is available for each particular card for interface configuration information. This section provides several examples to demonstrate how to configure line cards using both the global configuration mode and the setup facility.

Configuring a POS Line Card

To configure a POS line card, perform the following procedure. The IP address and subnet mask are examples only. You will need to obtain this information from your network administrator.

	Command	Purpose
Step 1	Router(config)# **interface pos 3/0**	Enters interface configuration mode on the POS interface located in slot 3 and port 0.
Step 2	Router(config-if)# **ip address 2.1.1.1 255.0.0.0**	Specifies the IP address and subnet mask for the interface.
Step 3	Router(config-if)# **no shutdown**	Changes the shutdown state to up and enables the interface. If you configure an interface using the command line interface, you must use this command to enable the interface. When you use the **setup** command facility, this is performed automatically.

Additional configuration tasks can be performed for the line card in interface configuration mode. Refer to the installation note provided with the line card for additional information.

Note By default, POS interfaces use the 32-bit cyclic redundancy check (CRC) and high-level data link control (HDLC) as the encapsulation protocol.

The following commands are also useful for configuring POS interfaces:

Command	Purpose
Router(config-if)# **pos scramble-atm**	Enables SONET payload scrambling on a POS interface.
Router(config-if)# **clock source internal**	Controls which clock a POS interface will use to clock its transmitted data.

The following sample excerpt from a **setup** command facility session for a 4-port OC-3c/STM-1c POS line card shows settings for a typical configuration:

```
Configuring interface POS3/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
  Configure IP unnumbered on this interface?: no
    IP address for this interface: 2.1.1.1
    Number of bits in subnet field: 0
    Class A network is 2.0.0.0, 0 subnet bits; mask is 255.0.0.0
  Configure CLNS on this interface?: yes
```

If additional configuration is required, use the global configuration mode as described at the beginning of this section.

Configuring an ATM Line Card

To configure an ATM line card, perform the following procedure. The IP address and subnet mask are examples only. You will need to obtain this information from your network administrator.

	Command	Purpose
Step 1	`Router(config)# interface atm 1/0`	Enters interface configuration mode on the ATM interface located in slot 3 and port 0.
Step 2	`Router(config-if)# ip address 1.1.1.2 255.0.0.0`	Specifies the IP address and subnet mask for the interface.
Step 3	`Router(config-if)# no shutdown`	Changes the shutdown state to up and enables the interface. If you configure an interface using the command line interface, you must use this command to enable the interface. When you use the **setup** command facility, this is performed automatically.

Additional configuration tasks can be performed for the line card in interface configuration mode. Refer to the installation note provided with the line card for additional information.

In the following example, an ATM line card is being configured to use IP.

```
Configuring interface ATM1/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
    IP address for this interface: 1.1.1.2
    Number of bits in subnet field: 0
    Class A network is 1.0.0.0, 0 subnet bits; mask is 255.0.0.0
```

Note You might have to configure additional parameters for the installed ATM line cards if you want to use all their capabilities. For example, additional steps are required to configure permanent virtual circuits (PVCs).

Route Processing

In Cisco IOS Release 12.0(22)S, the Performance Route Processor (PRP) was introduced to replace the Gigabit Route Processor (GRP). The PRP provides a faster processor, multilayer cache, improved fabric interface for faster communication between PRP and line cards, and larger memory capacity.

The PRP is designed to support all Cisco IOS software features that are supported on the GRP. Certain exceptions apply regarding High Availability. Refer to the *Cisco IOS Release 12.0S Release Notes* for more information regarding supported features.

For more information regarding the PRP, refer to the PRP Feature Module at the following location:

http://wwwicisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/prp htm

Redundant Route Processor Support

As of Cisco IOS Release 12.0(5)S, the Cisco 12000 Series Internet Router supports the installation of two route processors (RPs). One RP functions as the primary or active processor. The primary RP supports all normal RP operation. The other RP functions as the secondary or standby processor. The secondary RP monitors the primary and will take over normal RP operations if it detects a failure in the primary RP.

Note The redundant RP features are only supported when using two GRPs or two PRPs. There is no support for redundancy when a GRP is used together with a PRP.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/gsr_rp.htm

Route Processor Redundancy Plus (RPR+)

An enhancement to RP redundancy called Route Processor Redundancy Plus (RPR+) was introduced in Cisco IOS Releases 12.0(17ST) and 12.0(22)S. With RPR+, the standby RP is fully initialized and configured. This feature allows RPR+ to dramatically shorten the switchover time if the active RP fails or if a manual switchover is performed. Because both the startup configuration and the running configuration are continually synchronized from the active to the standby RP, line cards are not reset during a switchover. The interfaces remain up during this transfer, so neighboring routers do not detect a link flap (that is, the link does not go down and back up).

Note RPR+ features are only supported when using two GRPs or two PRPs. There is no support for redundancy when a GRP is used together with a PRP.

The default redundancy mode for Cisco 12000 Series Internet Routers is standard RPR. For information on configuring RPR+, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st17/rpr_plus.htm

RPR+ is not supported on all Cisco 12000 Series Internet Router line cards. Refer to the *Release Notes for Cisco IOS Release 12.0S* for the list of supported line cards.

Cisco Nonstop Forwarding

Cisco Nonstop Forwarding (NSF) is a complementary feature to the Stateful Switchover (SSO) feature in Cisco IOS software. NSF always runs together with SSO and works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover.

Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

NSF allows data packets to continue forwarding along known routes while the routing protocol information is being restored following a switchover. With NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

For information about the SSO feature, refer to this url:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/sso120s.htm

For more information about Cisco NSF, refer to the Cisco Nonstop Forwarding document at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/nsf120s.htm

PCMCIA Flash Memory Tasks

The linear Flash memory card or Flash disk that shipped with your router contains the default Cisco IOS software image you need to boot your router. Flash disks provide higher capacity and better performance than linear Flash memory cards, but otherwise they function almost the same. When using a linear Flash memory card, the Cisco IOS command to identify and access the card is **slot0:** or **slot1:**, depending on the PCMCIA slot in use. When using a Flash disk, those commands are replaced with **disk0:** or **disk1:**.

Note Use only Type I or Type II Flash memory cards.

The following sections describe common software tasks that involve Flash memory cards and Flash disks.

- Formatting a Flash Memory Card or Flash Disk, page 2-11
- Booting from Flash Memory, page 2-12
- Manipulating Files on a Flash Memory Card or Flash Disk, page 2-13

Note For information regarding available Flash memory cards and Flash disks, and how to install them into the RP on your router, refer to the installation and configuration guide available for your Cisco 12000 Series Internet Router.

Formatting a Flash Memory Card or Flash Disk

Before you can use a new Flash memory card or Flash disk, you must format it.

Caution The procedure erases all information on a Flash memory card. To prevent the loss of important data that might be stored on a Flash memory card, proceed carefully. If you want to save the data contained on a Flash memory card, copy the data to a server before you format the card.

To format a new Flash memory card or Flash disk in the RP, follow these steps:

	Command	Purpose

Step 1	`Router#` **`format slot0:`**
	`or`
	`Router#` **`format disk0:`**
		Formats a new Flash memory card or Flash disk located in slot 0 on the RP. If the card or disk is located in slot 1, use the **slot1:** or **disk1:** keyword.

Step 2	`All sectors will be erased, proceed? [confirm]` **`y`**	Confirms the card or disk format.

Step 3	`Enter volume id (up to 30 characters):` **`MyNewCard`**
	`Formatting sector` *`n`*
	`Format device slot0 completed`
		Assigns the specified volume ID to the card or disk (MyNewCard in this example). The console displays the “Formatting sector n” line as the card or disk is being formatted. When the count reaches 1, the formatting process is complete.

The new linear Flash memory card or Flash disk is now formatted and ready to use.

For complete command descriptions and configuration information, refer to the *Configuration Fundamentals Command Reference* located at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/index.htm

or the *Configuration Fundamentals Configuration Guide* located at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/index.htm.

Booting from Flash Memory

To enable booting from a Cisco IOS software image file located on a PCMCIA Flash memory card or Flash disk, follow these steps:

	Command	Purpose

Step 1	`Router#` **`configure terminal`**
	`Enter configuration commands, one per line. End with CNTL/Z.`
		Enters global configuration mode.

Step 2	`Router(config)#` **`boot system flash slot0:`***`filename`*	Specifies that at startup, the router loads the software image named *filename*, located on the linear Flash memory card in slot 0. Use **slot1:** for a Flash memory card in slot 1, **disk0:** for a Flash disk in slot 0, and **disk1:** for a Flash disk in slot 1.
Step 3	`Router(config)#` **`config-register 0x0102`**	Disables the Break function and enables the **boot system flash** command.
Step 4	`Router(config)#` **`Ctrl-z`**	Exits global configuration mode.

Step 5	`Router#` **`copy running-config startup-config`**
	`or`
	`Router#` **`write memory`**
		Saves the software configuration register settings to NVRAM.

Step 6	`Router#` **`reload`**	Reboots the router and uses the specified image on the Flash memory card inserted in PCMCIA slot 0 to boot the system.

Note By default, the router boots from a software image file on a Flash memory card or Flash disk located in slot 0.

Manipulating Files on a Flash Memory Card or Flash Disk

You can copy and move files to and from Flash memory cards and Flash disks as you would to any file system. Use any of the following commands to manipulate files on Flash memory cards or Flash disks.

Command	Purpose
`Router# pwd`	Displays the current setting of the **cd** command. Use this command to determine whether the present working directory you are accessing is the onboard Flash SIMM on the RP or a PCMCIA Flash memory device in a slot on the RP. If the router returns *slot0:*, this indicates that you are accessing a PCMCIA linear Flash memory card inserted in slot 0 of the RP.
`Router# cd slot1:`	Changes the present working directory you are accessing to the PCMCIA linear Flash memory card inserted in slot 1 of the RP. Use **disk1:** to access a Flash disk located in slot 1 of the RP.
`Router# cd bootflash:`	Changes the present working directory you are accessing to the Flash memory SIMM on the RP.
`Router# dir`	Displays the directory contents of the Flash memory media in use.
`Router# delete slot0:filename`	Deletes the file *filename* from a linear Flash memory card in slot 0. Use **slot1:** for a card in slot 1, **disk0:** for a disk in slot 0, and **disk1:** for a disk in slot 1. Files that are deleted are removed from the directory list, but are not erased permanently. You can use the **undelete** command to recover deleted files.
`Router# squeeze slot0:`	Permanently removes deleted files from a linear Flash memory card located in slot 0. The **squeeze** command also makes all other undeleted files on the Flash card contiguous. Use **slot1:** for a card in slot 1. The squeeze command is not necessary when using Flash disks.

Upgrading and Backing Up Cisco IOS Software Images and Configuration Files

The following sections describe common software tasks that involve upgrading and backing up files on your router:

- Upgrading a Cisco IOS Software Image on Flash Memory from a TFTP Server, page 2-14
- Copying Cisco IOS Software Images Between Flash Memory Cards or Flash Disks, page 2-15
- Specifying a Cisco IOS Software Image File as the Default Boot Image, page 2-16
- Upgrading the Boot Image in SIMM (Bootflash), page 2-17
- Saving a Configuration File, page 2-18
- Restoring a Configuration File, page 2-19
- Recovering from Locked Blocks in Flash Memory Cards or Flash Disks, page 2-19

Upgrading a Cisco IOS Software Image on Flash Memory from a TFTP Server

Your router is shipped with a default Cisco IOS software image preloaded into the Flash memory card or Flash disk located in slot 0 of the RP. As future releases of Cisco IOS software become available, you can download them from Cisco.com to upgrade your router software. You can save these image files to a TFTP server on your network and subsequently download them to the routers on your network.

Note Flash memory cards and Flash disks must be formatted before they are used for the first time. If you have not formatted the Flash memory card or Flash disk, see the "Formatting a Flash Memory Card or Flash Disk" section on page 2-11.

Note To avoid a situation where the router does not have a valid Cisco IOS software image to boot from, make sure that you retain the current software image on the Flash memory card or disk. If you do not have room on the Flash memory card for a second image, save a copy of the image on a separate Flash memory card or Flash disk, or on a TFTP server on your network. See the "Copying Cisco IOS Software Images Between Flash Memory Cards or Flash Disks" section on page 2-15.

To upgrade a Cisco IOS software image file on Flash memory from a TFTP server, follow these steps:

	Command	Purpose
Step 1	`Router# `**`show slot0:`**	Verifies that there is sufficient room on the Flash memory card or Flash disk to copy the new software image. Default Flash memory cards are 20M in size. If you see that there is sufficient room for the image that you are copying, continue with the **copy** command in Step 4. Otherwise, continue with the next step.

Step 2	`Router# `**`delete slot0:`***`filename`*
	or
	`Router# `**`delete disk0:`***`filename`*
		For Flash memory cards, (**slot0:** syntax) marks the file *filename* to be deleted; for Flash disks, (**disk0:** syntax) deletes the file *filename*. Delete enough files so that there will be sufficient space on the Flash memory card or Flash disk for the new software image. If you need the files for future use, be sure to copy them to another storage media before you delete them.

Step 3	`Router# `**`squeeze slot0:`**	Permanently removes deleted files from a Flash memory card located in slot 0. The **squeeze** command also makes all other undeleted files on the Flash card contiguous. This step is not required if you are using a Flash disk.
Step 4	`Router# `**`copy tftp: slot0:`**	Begins the copy dialog to copy a file from a TFTP server to a linear Flash memory card located in slot 0 of the RP. Use **slot1:** to copy to a linear Flash memory card in slot 1, **disk0:** to copy to a Flash disk in slot 0, and **disk1:** to copy to a Flash disk in slot 1.
Step 5	`Address or name of remote host []? `**`192.168.16.254`**	Specifies the address of the TFTP server from which to copy the Cisco ISO software image. The IP address specified here is an example only.
Step 6	`Source filename []? `**`gsr-p-mz.120-7.4.5`**	Specifies the name of the file containing the Cisco ISO software image. In this example, the file is named gsr-p-mz.120-7.4.5.

	Command	Purpose
Step 7	Destination filename [gsr-p-mz.120-7.4.5]? **<Return>**	Specifies the name of the file to be created on the Flash memory media. Press **Return** to use the same name as the source file. After you enter the name of the destination file, the router begins to copy the file. When the privileged EXEC prompt is displayed (`Router#`), the copy is complete.
Step 8	Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z.	Enters global configuration mode.
Step 9	Router(config)# **boot system flash slot0:gsr-p-mz.120-7.4.5**	Specifies that at startup, the router loads the software image named gsr-p-mz.120-7.4.5, located on the Flash memory card in slot 0.
Step 10	Router(config)# **config-register 0x0102**	Disables the Break function and enables the **boot system flash** command (specified in the previous Step).
Step 11	Router(config)# **Ctrl-Z**	Exits global configuration mode.
Step 12	Router# **copy running-config startup-config** or Router# **write memory**	Saves the software configuration register settings to NVRAM.
Step 13	Router# **reload**	Reboots the router and uses the specified image on the Flash memory card inserted in PCMCIA slot 0 to boot the system.

This completes the Cisco IOS software upgrade procedure.

Note If there is not enough room on the Flash memory card or Flash disk to perform the copy, an error message is displayed to the console. In this case, you will need to delete more files to make room for the new software image, as described in Step 2 and Step 3 of the procedure above.

Copying Cisco IOS Software Images Between Flash Memory Cards or Flash Disks

You can store a Cisco IOS software image on a Flash memory card or Flash disk for backup purposes. You can then copy the software image to the Flash memory card or Flash disk that you are using in your router.

Note Flash memory cards and Flash disks must be formatted before they are used for the first time. If you have not formatted the Flash memory card or Flash disk, see the "Formatting a Flash Memory Card or Flash Disk" section on page 2-11.

Note Copying images between flash memory cards can take a long time.

To copy a Cisco IOS software image file from one Flash memory card or Flash disk to another, follow these steps:

	Command	Purpose
Step 1	Router# **copy slot1: slot0:**	Begins the copy dialog to copy a file on Flash memory card located in slot 1 to the Flash memory card located in slot 0. Use **disk0:** to copy to or from a Flash disk in slot 0, and **disk1:** to copy to or from a Flash disk in slot 1.
Step 2	Source filename []? **gsr-p-mz.120-7.4.5**	Specifies the name of the file containing the Cisco ISO software image on slot 1. In this example, the file is named gsr-p-mz.120-7.4.5.
Step 3	Destination filename [gsr-p-mz.120-7.4.5]? **<Return>**	Specifies the name of the file to be created on the Flash memory card in slot 0. Press **Return** to use the same name as the source file. After you enter the name of the destination file, the router begins to copy the file. This procedure can take a very long time. When the privileged EXEC prompt is displayed (Router#), the copy is complete.

Note If there is not enough room on the Flash memory card or Flash disk to perform the copy, an error message is displayed to the console. In this case, you will need to delete files to make room for the new software image, as described in the "Upgrading a Cisco IOS Software Image on Flash Memory from a TFTP Server" section on page 2-14.

To designate the copied image file to be the new default system image for boot purposes, see the "Specifying a Cisco IOS Software Image File as the Default Boot Image" section on page 2-16.

Specifying a Cisco IOS Software Image File as the Default Boot Image

After you copy a Cisco IOS software image file to a Flash memory card or Flash disk, you will want to designate this new file as the new default system image for boot purposes. To do this, follow these steps:

	Command	Purpose
Step 1	Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z.	Enters global configuration mode.
Step 2	Router(config)# **boot system flash slot0:gsr-p-mz.ME12_SRP_VER_12_08_12**	Specifies that at startup, the router loads the software image named gsr-p-mz.ME12_SRP_VER_12_08_12, located on the linear Flash memory card in slot 0.
Step 3	Router(config)# **config-register 0x0102**	Disables the Break function and enables the **boot system flash** command.
Step 4	Router(config)# **Ctrl-Z**	Exits global configuration mode.
Step 5	Router# **copy running-config startup-config** or Router# **write memory**	Saves the software configuration register settings to NVRAM.
Step 6	Router# **reload**	Reboots the router and uses the specified image on the Flash memory card inserted in PCMCIA slot 0 to boot the system.

Upgrading the Boot Image in SIMM (Bootflash)

A mini-Cisco IOS software image is preloaded into the single inline memory module (SIMM) or bootflash. This image can be used to boot the router if there is no other valid image available. It provides a limited number of configuration commands that you can use to locate a valid Cisco IOS software image or correct basic configuration problems. This image provides no routing capabilities.

Caution You must have a valid copy of a boot image in the onboard Flash memory SIMM (bootflash) in order to boot the router. If you delete the current version of the boot image, you must copy in a new image before you reboot the router.

If it becomes necessary to upgrade this image, download a new image from Cisco.com. Use the following procedure to upgrade the boot image in the bootflash with the new image:

Step 1	`Router#` **`delete bootflash:gsr-boot-mz.120-8.S`**	Deletes the current bootflash image from the bootflash. In this example, the name of the image is *gsr-boot-mz.120-8.S*. Since there is generally not enough room in the bootflash for more than one image, you will need to delete the current image before you can copy in a new one. If you attempt the copy and there is not enough room in the bootflash for the image, an error message will be displayed.
Step 2	`Router#` **`squeeze bootflash:`**	Permanently deletes all files in the bootflash that are marked as deleted.
Step 3	`Router#` **`copy tftp: bootflash:`**	Begins the copy dialog to copy a file from a TFTP server to the online Flash memory SIMM (bootflash).
Step 4	`Address or name of remote host []?` **`192.168.16.254`**	Specifies the address of the TFTP server from which to copy the Cisco ISO software image.
Step 5	`Source filename []?` **`gsr-boot-mz.120-21.S`**	Specifies the name of the file containing the boot image. In this example, the file is named gsr-boot-mz.120-21.S.bin.

Step 6	`Destination filename [gsr-boot-mz.120-21.S]?`
	`<Return>`
		Specifies the name of the file to be created on the Flash memory media. Press **Return** to use the same name as the source file. After you enter the name of the destination file, the router begins to copy the file. When the privileged EXEC prompt is displayed (Router#), the copy is complete.

Step 7	`Router#` **`reload`**	Reboots the router. The new bootflash image is now ready to be used.

Note Instead of using the **delete** and **squeeze** commands in Step 1 and Step 2, you can use the **format bootflash:** command. Note, however, that the **format** command deletes all crashinfo files located in the bootflash.

This completes the procedure for upgrading the boot image in the onboard Flash memory SIMM.

Saving a Configuration File

It is a good practice to save your configuration file, in case you need to restore it for any reason. You should save your configuration file before you make major changes to the configuration. You have two configuration files: the startup configuration file located in NVRAM and the running configuration file located in DRAM. These will generally be the same, unless you are in the process of changing the configuration.

To save your startup configuration file, use one of the following commands, depending on where you want to save the file:

Command	Purpose
`Router# copy startup-config slot0:filename`	Copies the configuration file located in NVRAM (the system default) to the PCMCIA Flash memory card in slot 0.
`Router# copy startup-config slot1:filename`	Copies the configuration file located in NVRAM (the system default) to the PCMCIA Flash memory card in slot 1.
`Router# copy startup-config disk0:filename`	Copies the configuration file located in NVRAM (the system default) to the PCMCIA Flash memory disk in slot 0.
`Router# copy startup-config disk1:filename`	Copies the configuration file located in NVRAM (the system default) to the PCMCIA Flash memory disk in slot 1.
`Router# copy startup-config tftp:`	Copies the configuration file located in NVRAM (the system default) to a TFTP server on the network. You will be prompted to provide the address of the TFTP server and the file name.

To save your running configuration file, use one of the following commands, depending on where you want to save the file:

Command	Purpose
`Router# copy running-config slot0:filename`	Copies the configuration file located in DRAM (the system default) to the PCMCIA Flash memory card in slot 0.
`Router# copy running-config slot1:filename`	Copies the configuration file located in DRAM (the system default) to the PCMCIA Flash memory card in slot 1.
`Router# copy running-config disk0:filename`	Copies the configuration file located in DRAM (the system default) to the PCMCIA Flash memory disk in slot 0.
`Router# copy running-config disk1:filename`	Copies the configuration file located in DRAM (the system default) to the PCMCIA Flash memory disk in slot 1.
`Router# copy running-config tftp:`	Copies the configuration file located in DRAM (the system default) to a TFTP server on the network. You will be prompted to provide the address of the TFTP server and the file name.

Use the **dir** command to verify that the configuration file was copied correctly to the Flash memory media, as shown in the following example for the Flash memory card in slot 0:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  May 10 1997 19:24:12 gsr-p-mz.112-8
3   1215     May 10 1997 20:30:52 myfile1
4   6176844  May 10 1997 23:04:10 gsr-p-mz.112-8.1
5   1186     May 10 1997 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
```

Restoring a Configuration File

To restore a configuration file from a Flash memory card or disk in PCMCIA slot 0 or slot 1 to NVRAM, follow these steps:

	Command	Purpose
Step 1	Router# **copy slot0:***filename* **startup-config**	Copies the configuration file located in the PCMCIA Flash memory card in slot 0 to NVRAM (the system default). Use **slot1:** to copy from a card in slot 1, **disk0:** to copy from a disk in slot 0, **disk1:** to copy from a disk in slot 1.
Step 2	Router# **copy startup-config running-config**	Designates the startup configuration file stored in NVRAM to be the default running configuration file for the system.

This completes the procedure for restoring a configuration file from a Flash memory card or disk to NVRAM.

Recovering from Locked Blocks in Flash Memory Cards or Flash Disks

A locked block in a Flash memory card or Flash disk occurs when power is lost or a Flash memory card or Flash disk is removed from its PCMCIA slot on the RP during a write or erase operation.

When a block of Flash memory is locked, it cannot be written to or erased. Any attempt at such an operation will consistently fail at the blocked location. The only way to recover from locked blocks in a Flash memory card or Flash disk is to reformat it using the **format** command. For more information, see the "Formatting a Flash Memory Card or Flash Disk" section on page 2-11.

Caution Formatting a Flash memory card or disk erases all existing data on the card or disk.

CHAPTER 3

Additional Configuration Tasks for the Cisco 12000 Series Internet Router

This chapter describes additional configuration and troubleshooting tasks for the Cisco 12000 Series Internet Router. It discusses the following subjects:

- Configuration Tasks, page 3-1
- Troubleshooting Tips, page 3-7
- Monitoring and Maintaining the Cisco 12000 Series Internet Router, page 3-11

Configuration Tasks

This section details additional configuration tasks that may need to be performed on your router. The following items are described:

- The Software Configuration Register, page 3-1
- Recovering a Lost Password, page 3-6
- Useful Configuration Commands, page 3-7

The Software Configuration Register

Configuring the software configuration register is described in the following sections:

- Description of the Software Configuration Register, page 3-1
- Boot Field Settings, page 3-3
- Configuring the Software Configuration Register, page 3-4
- Bits in the Software Configuration Register, page 3-4

Description of the Software Configuration Register

The software configuration register is a 16-bit register in NVRAM that you use to define specific system parameters. You can set or change the contents of this register to accomplish the following tasks:

- Define the source for the default Cisco IOS software. You can specify any of the following:
  - Flash memory card inserted in PCMCIA slot 0

  - TFTP server on the network
  - Flash memory SIMM (NVRAM) on the RP
  - Boot image stored within the operating environment, which you access by using an appropriate form of the **boot** command entered at the ROM monitor prompt (`rommon>`)
- Define a default boot filename.
- Enable or disable the Break function.
- Control broadcast addresses.
- Set the console terminal baud rate.
- Recover a lost password.
- Force an automatic boot using a boot image.

  When you first power on the router, a boot image called the RP ROM monitor is executed, resulting in the display of the ROM monitor prompt (`Rommon>`). At this prompt, you have access to a limited set of commands that enable you to set values in the software configuration register and to perform a number of other tasks.

  The RP ROM monitor is loaded into the RP Flash ROM when the RP is manufactured. You can use it to boot the system from local Flash memory devices. The RP ROM monitor software can be upgraded in the field, if necessary.
- Read **boot system** commands from the configuration file stored in NVRAM.

Table 3-1 defines the bits in the software configuration register.

Table 3-1 Software Configuration Register Bit Meanings

Bit Number[1]	Hexadecimal Value	Meaning/Function
00 to 03	0x0000 to 0x000F	Comprises the boot field for defining the source of a default Cisco IOS software image required to run the router (see Table 3-2)
06	0x0040	Causes system software to ignore the contents of NVRAM
07	0x0080	Enables the OEM[2] bit
08	0x0100	Disables the Break function
09	0x0200	Uses a secondary bootstrap
10	0x0400	Broadcasts Internet Protocol (IP) with all zeros
11 and 12	0x0800 to 0x1000	Defines the console baud rate (the default setting is 9600 bps)
13	0x2000	Boots the default Flash memory software if the network boot fails
14	0x4000	Excludes network numbers from IP broadcasts
15	0x8000	Enables diagnostic messages and ignores the contents of NVRAM

[1] The factory default value for the software configuration register is 0x0102. This value is a combination of binary bit 8 = 0x0100 and binary bits 00 through 03 = 0x0002.

[2] OEM = original equipment manufacturer.

Note Valid software configuration register values may be combinations of settings, rather than the individual settings listed in Table 3-1. For example, the factory default value 0x0102 for the software configuration register is actually a composite of several settings.

Boot Field Settings

Bits 00 to 03 of the software configuration register are referred to as the boot field, which defines a source for booting the default Cisco IOS software image required to run the router. The value of the boot field is specified as a binary number, as described in Table 3-2.

Table 3-2 Definition of Bits in Boot Field of Software Configuration Register

Boot Field	Meaning
00	On power up, the system remains at the ROM monitor prompt (`rommon>`), awaiting a user command to boot the system manually. See the "Manually Booting from a Cisco IOS Software Image" section on page 2-2.
01	On power up, the system automatically boots the first system image found in the onboard Flash memory SIMM on the RP.
02 to 0F	If a valid **boot system** command is stored in the NVRAM configuration file, the router boots the Cisco IOS software image as directed by that value. If no **boot system** command is present in the configuration file, the router forms a default boot filename and attempts to acquire that file from a network TFTP server. To compute the filename of this default image, the router starts with *cisco* and appends the octal equivalent of the boot field value, a hyphen, and the processor type (grp or prp). Table 3-3 lists the range of possible computed default filenames for booting over the network. The router would use one of these filenames to boot a default system image stored on a network TFTP server. If the configuration file contains a valid **boot system** configuration command, the system uses these instructions to boot the system, rather than using the filename it computed from the software configuration register settings. For this setting, it is assumed that the Ethernet port on the RP is configured and operational. **Note** If a bootable Cisco IOS software image exists in a Flash memory card inserted in PCMCIA slot 0 or slot 1, the software configuration register boot field setting is overridden, and the system boots from the Cisco IOS software image in the Flash memory card, rather than from a network TFTP image.

Note Cisco 12000 Series Internet Routers are typically delivered from the factory with a mini-Cisco IOS software boot image in the boot flash and a flash card containing a suitable working Cisco IOS image. If you discover that you need a Cisco IOS upgrade, you should download the appropriate Cisco IOS image from Cisco.com. Refer to the "Upgrading and Backing Up Cisco IOS Software Images and Configuration Files" section on page 2-13.

Configuring the Software Configuration Register

To configure the software configuration register, follow these steps:

	Command	Purpose

Step 1	`Router>` **`enable`**
	`Password: <password>`
		Enters privileged EXEC mode.

Step 2	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 3	`Router(config)#` **`config-register 0x`***`value`*	Sets the contents of the software configuration register, where `value` is a 4-bit hexadecimal number as described in Table 3-1.
Step 4	`Router(config)#` **`ctrl-Z`**	Exits global configuration mode.
Step 5	`Router#` **`show version`**	Displays the software configuration register value currently in effect. This is the value that will be used the next time the router reloads. The value is displayed on the last line of the display, as in the following example: `Configuration register is 0x141 (will be 0x102 at next reload)`

Step 6	`Router#` **`copy running-config startup-config`**
	`or`
	`Router#` **`write memory`**
		Saves the software configuration register settings to NVRAM.

Step 7	`Router#` **`reload`**	Reboots the router. Configuration register changes take effect only after the system reloads.

Bits in the Software Configuration Register

As described in the "Boot Field Settings" section on page 3-3, the boot field setting determines the source of the Cisco IOS software image that is used to boot the router. A detailed description of the bit values for the boot field and their associated action or filename is given in Table 3-3

Table 3-3 Default Boot Filenames

Action/Filename	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
Default software	0	0	0	1
cisco2-grp or cisco2-prp	0	0	1	0
cisco3-grp or cisco3-prp	0	0	1	1
cisco4-grp or cisco4-prp	0	1	0	0
cisco5-grp or cisco5-prp	0	1	0	1
cisco6-grp or cisco6-prp	0	1	1	0
cisco7-grp or cisco7-prp	0	1	1	1
cisco10-grp or cisco10-prp	1	0	0	0
cisco11-grp or cisco11-prp	1	0	0	1
cisco12-grp or cisco12-prp	1	0	1	0
cisco13-grp or cisco13-prp	1	0	1	1
cisco14-grp or cisco14-prp	1	1	0	0

Table 3-3 Default Boot Filenames (continued)

Action/Filename	Bit 3	Bit 2	Bit 1	Bit 0
cisco15-grp or cisco15-prp	1	1	0	1
cisco16-grp or cisco16-prp	1	1	1	0
cisco17-grp or cisco17-prp	1	1	1	1

The remaining bits in the software configuration register are described following:

Bit 8 of the software configuration register controls the console Break key. Setting bit 8 causes the system to ignore the console Break key. This is the factory default. Conversely, clearing bit 8 causes the system to interpret a Break keystroke as a command to halt normal system operation and force the system into ROM monitor mode. Regardless of the setting of the Break enable bit in the software configuration register, pressing the Break key during approximately the first 5 seconds of booting causes a return to the ROM monitor.

Bit 9 is not used.

Bit 10 of the software configuration register controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros in the host portion of the IP broadcast address; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the IP broadcast address.

Table 3-4 shows the combined effect of bits 10 and 14.

Table 3-4 Configuration Register Settings for Broadcast Address Destination

Bit 14	Bit 10	Address (<net> <host>)
Off	Off	<ones> <ones>
Off	On	<zeros> <zeros>
On	On	<net> <zeros>
On	Off	<net> <ones>

Bits 11 and 12 of the software configuration register determine the data transmission rate of the console terminal. Table 3-5 shows the bit settings for the four available data transmission rates. The factory-set default data transmission rate is 9600 bps.

Table 3-5 System Console Terminal Data Transmission Rate Settings

Bit 12	Bit 11	Data Transmission Rate (bps)
0	0	9600
0	1	4800
1	0	1200
1	1	2400

Bit 13 of the software configuration register determines the system's response to a bootload failure. Setting bit 13 causes the system to load Cisco IOS software from Flash memory after five unsuccessful attempts to load a boot file from the network TFTP server. Clearing bit 13 causes the system to continue attempting to load a boot file from the network TFTP server indefinitely. Bit 13 in the software configuration register is set to 0 as the default at the factory.

Recovering a Lost Password

Note If the enable password is encrypted, the following procedure will not work for password recovery, and you will have to reconfigure the system before attempting a reboot. To reconfigure the system, use the displayed configuration, which is shown using the **show startup-config** command in privileged EXEC mode.

Before you begin the procedure to recover a lost password, you must attach an ASCII terminal to the RP console port and configure the terminal to operate at the same settings as the console port (usually 9600 bps, 8 data bits, no parity, and 2 stop bits). After you correctly connect the terminal to the console port, continue with the following steps to recover a lost password:

	Command	Purpose
Step 1	Router# **show version**	Displays the existing software configuration register value. The current configuration setting appears in the last line of the display output. Record this value for use in Step 9.
Step 2	Router# **reload** **Break key** or **Ctrl-]**	Enters ROM monitor mode. You must press the **Break** key or **Ctrl-]** within 5 seconds of the router turning on.
Step 3	rommon 1> **config-register** Configuration Summary enabled are: console baud: 9600 boot: image specified by the boot system command or default to: cisco2-prp do you wish to change the configuration? y/n [n]: **y** enable “diagnostic mode”? y/n [n]: enable “use net in IP bcast address”? y/n [n]: enable “load rom after netbootfails”? y/n [n]: enable “use all zero broadcast”? y/n [n]: enable “break/abort has effect?” y/n [n]: enable “ignore system config info?” [n]: **y** change console baud rate? y/n [n]: change boot characteristics? y/n [n] Configuration Summary enabled are: console baud: 9600 boot: image specified by the boot system command or default to: cisco2-prp do you wish to change the configuration? y/n [n] You must reset or power cycle for the new config to take effect	Sets the software configuration register to ignore the configuration file information. Answer **yes** to the following prompts: • do you wish to change the configuration? • enable “ignore system config info?”
Step 4	rommon 2> **initialize**	Initializes the router. The router goes through a power cycle; the software configuration register is set to ignore the configuration file; the router boots the system image and displays the system configuration dialog.

	Command	Purpose
Step 5	--- System Configuration Dialog --- Continue with configuration dialog? [yes/no]: **n** Press RETURN to get started!	Exits the system configuration dialog. You must answer **no** to continue with the configuration dialog and then press **Return** to exit the configuration dialog.
Step 6	Router> **enable** Password: *<password>*	Enters privileged EXEC mode.
Step 7	Router# **show startup-config**	Displays the enable password in the configuration file.
Step 8	Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z.	Enters global configuration mode.
Step 9	Router(config)# **config-register 0x***value*	Changes the software configuration register value back to its original value, where value is the hexadecimal number noted in Step 1.
Step 10	Router(config)# **Ctrl-z**	Exits global configuration mode.
Step 11	Router# **reload**	Reboots the router. You should now be able to use the recovered password with the **enable** command to gain access to the router.

Useful Configuration Commands

The following are additional commands that are useful in configuring your router:

Command	Purpose
Router# **attach** *slot-number*	Accesses the Cisco IOS software image on a line card to monitor and maintain information on the line card. To exit from the Cisco IOS software image on the line card and return to the Cisco IOS image on the RP card, use the **exit** command.
Router# **execute on** {**slot** *slot-number* | **all**} *command*	Executes commands remotely on a line card.
Router(config)# **microcode slot** *slot-number* {**flash** *file-id* | **tftp** *file-id*}	Loads a Cisco IOS software image on a line card from Flash memory or a TFTP server.
Router(config)# **microcode reload** *slot-number*	Reloads the Cisco IOS image on a line card on a Cisco 12000 Series Internet Router after all microcode configuration commands have been entered.
Router# **hw-module slot** *slot-number* **reload**	Reloads the line card. This causes the line card to reset and redownload the Maintenance Bus (MBus) and Fabric Downloader software modules before attempting to redownload the line card Cisco IOS software.

Troubleshooting Tips

This section contains information for diagnosing faulty hardware cards and troubleshooting router crash information. It contains the following sections:

- Field Diagnostics, page 3-8

Field Diagnostics

Field diagnostics are available for the Cisco 12000 Series Internet Router to help you isolate faulty hardware to the level of a field-replaceable unit (FRU) without disrupting the operation of the system. After you identify the faulty unit, you can replace it with a spare unit.

Field diagnostics are not designed to identify specific components within the router. They simply determine whether a particular card is operational or defective.

Starting with Cisco IOS Release 12.0(22)S, Cisco Systems has unbundled the Cisco 12000 Series Internet Router field diagnostics line card image from the IOS image. In earlier versions, diagnostics could be launched from the command line and the embedded image would be launched. To accommodate customers with 20-MB Flash memory cards, line card field diagnostics are now stored and maintained as a separate image that must be available on a Flash memory card or a TFTP boot server before the field diagnostics commands can be used. Router processor and switch fabric field diagnostics continue to be bundled and need not be launched from a separate image.

Field diagnostics images are approximately 18 MB in size. IOS images are slightly larger. A single 64-MB Flash memory card can contain both images, or these images can be stored individually on two 20-MB memory cards in PCMCIA slots 0 and 1. To accomodate future feature releases, it is recommended that you use the larger Flash memory disks.

The diagnostics image is named **c12k-fdiagsbflc-mz.***120-25.S* and is always available on Cisco.com. 120-25.S is the version number of the image that corresponds to the Cisco IOS image, in this example: 12.0(25)S.

Caution Performing field diagnostics on a line card stops all activity on the line card. Before the **diag** command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

To perform field diagnostics on your router, use one of the following commands:

Command	Purpose
`Router# diag slot-number source tftp tftp://192.168.2.2/c12k-fdiagsbflc.120-22.S`	Performs field diagnostics on the line card in slot *slot-number*, using the image contained at the specified TFTP site. The file name in this example is a sample only; you must use a valid image file.
`Router# diag slot-number source flash slot0:/c12k-fdiagsbflc.120-22.S`	Performs field diagnostics on the line card in slot *slot-number*, using the image contained on the Flash memory card located in slot 0. The file name in this example is a sample only; you must use a valid image file.
`Router# diag slot-number previous`	Displays previous test results (if any exist) for the card. This option is only available for line cards and RPs.
`Router# diag slot-number halt`	Stops the field diagnostic testing on the line card. This option is only available for line cards and RPs.
`Router# diag slot-number`	Performs field diagnostics on a SFC or CSC in slot *slot-number*. The image is included with the standard Cisco IOS software and does not need to be available from an external source.

Additional keywords can be used with the **diag** command to limit the output or amount of testing performed. For more information, see the "diag" section on page 4-6. Field diagnostics are described more fully in the document *Field Diagnostics for the Cisco 12000 Series Internet Router* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/diag.htm

Upgrading the FPGA Image on a Line Card

If a line card does not boot and you receive an error message indicating that there is a problem with the field-programmable gate array (FPGA) image, or if the line card alphanumeric LED display remains frozen in IOS STRT state, you need to upgrade the FPGA image using the **diag** command.

Note The Cisco IOS image running on the router has an associated FPGA image that is identified by a version number. The major version number of the FPGA image must match the FPGA image version defined in the Cisco IOS image; the minor version number on the FPGA image must be the same as or greater than the minor version numbers on the FPGA image defined in the Cisco IOS image. For example, if the Cisco IOS image specifies a minimum FPGA image of 03.02, the software will verify that the actual major version number of the FPGA image in the line card bootflash is 03, and that the minor version number is 02 or above.

To upgrade the FPGA image on a line card, follow these steps:

	Command	Purpose
Step 1	Router> **enable** Password: <password>	Enters privileged EXEC mode.
Step 2	Router# **diag** *slot-number* **update-fpga source** {**tftp** | **flash**} *source-path*	Updates flash memory with field-programmable gate array (FPGA) image(s) from the current field diagnostics download image. The name of the image file is **c12k-fdiagsbflc-mz.***120-25.S* where 120-25.S is the version number. For Flash cards, the source path would typically be **slot0:c12k-fdiagsbflc-mz.***120-25.S* or **slot1:c12k-fdiagsbflc-mz.***120-25.S*. The TFTP source path would typically be: **tftp://***tftp_server_ip_address/my_directory***/c12k-fdiagsbflc-mz.***120-25.S*. **Note** Do not unplug the line card or terminate the field diagnostics session during this test.

Retrieving Information from the Crashinfo File

The crashinfo file is a collection of useful information related to the most recent router crash. When a router crashes as a result of data or stack corruption, additional reload information required to debug this type of crash can be found in the crashinfo file. By default, the crashinfo file is stored in the onboard Flash memory SIMM or bootflash under the name "crashinfo".

Use any of the following commands to obtain information about or display the contents of the crashinfo file:

Command	Purpose
Router# **show stack**	Displays information about the crashinfo file located in the bootflash. If a crashinfo file exists, at the end of the **show stack** output is a section called Information of Last System Crash that contains the name of the crashinfo file.
Router# **dir bootflash:** or Router# **dir sec-bootflash:**	Lists the contents of the bootflash. If a crashinfo file exists, it will be listed. Only the last crashinfo file is listed.
Router# **more bootflash: crashinfo_20000323-061850**	Displays more information about the specific crashinfo file.
Router# **dir /all bootflash:**	Lists the entire contents of the bootflash, including previous crashinfo files that have been marked as deleted. You can use the **undelete** command to restore older crashinfo files. However, before you can undelete an old crashinfo file, you must delete the most recent file. You can use the **squeeze** command on the bootflash to permanently delete old files.
Router# **show file bootflash:crashinfo**	Displays the contents of the most recent crashinfo file.
Router# **delete bootflash:crashinfo**	Marks the most recent crashinfo file as being deleted.
Router# **undelete** *file-index* **bootflash:**	Restores a deleted crashinfo file. The file-index is the number corresponding to the file you want to delete on the directory listing. Use the **dir bootflash:** command to view the file-index.
Router# **squeeze bootflash:**	Permanently deletes all files in the bootflash that are marked as deleted.

The following example illustrates how to view the contents of the bootflash, how to view the contents of the crashinfo file, and how to restore a previous crashinfo file and view its contents:

```
Router# show stack
...
    ***************************************************
    ******* Information of Last System Crash **********
    ***************************************************

    Using bootflash:crashinfo_20000323-061850. 2000
    CMD: 'sh int fas' 03:23:41 UTC Thu Mar 2 2000
    CMD: 'sh int fastEthernet 6/0/0' 03:23:44 UTC Thu Mar 2 2000
    CMD: 'conf t' 03:23:56 UTC Thu Mar 2 2000
    CMD: 'no ip cef di' 03:23:58 UTC Thu Mar 2 2000
    CMD: 'no ip cef distributed ' 03:23:58 UTC Thu Mar 2 2000
...

Router# dir bootflash:
    Directory of bootflash:/

      1  -rw-     4088008   Oct 07 1999 04:51:29  rsp-boot-mz.120-6.6
      2  -rw-      178619   Mar 23 2000 06:18:50  crashinfo_20000323-061850

    7602176 bytes total (3335292 bytes free)

Router# more bootflash:crashinfo_20000323-061850
     2000
    CMD: 'sh int fas' 03:23:41 UTC Thu Mar 2 2000
    CMD: 'sh int fastEthernet 6/0/0' 03:23:44 UTC Thu Mar 2 2000
    CMD: 'conf t' 03:23:56 UTC Thu Mar 2 2000
    CMD: 'no ip cef DI 03:23:58 UTC Thu Mar 2 2000
    CMD: 'no ip cef distributed ' 03:23:58 UTC Thu Mar 2 2000
    CMD: 'ip cef' 03:24:01 UTC Thu Mar 2 2000
...

Router# dir /all bootflash:
    -#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
    1   .. unknown  FD38E5C7  3FD81C   25  3921820 Oct 02 1998 14:43:56 rsp-boot-mz.112-15a.P.bin
    2   .D config   AF12EF9F  41C308    9   125547 Oct 16 1998 11:10:10 crashinfo
    3   .. config   33DEAF65  43A950    9   124360 Oct 16 1998 11:15:50 crashinfo

    3430064 bytes available (4172112 bytes used)

Router# show file bootflash:crashinfo

    Compliance with U.S. Export Laws and Regulations - Encryption

    This product performs encryption and is regulated for export
    by the US Government.

    .....  file continues here....
...
Router# dir /all bootflash:
    -#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
    1   .. unknown  FD38E5C7  3FD81C   25  3921820 Oct 02 1998 14:43:56 rsp-boot-mz.112-15a.P.bin
    2   .D config   AF12EF9F  41C308    9   125547 Oct 16 1998 11:10:10 crashinfo
    3   .. config   33DEAF65  43A950    9   124360 Oct 16 1998 11:15:50 crashinfo

    3430064 bytes available (4172112 bytes used)

Router# delete bootflash:crashinfo

Router# dir /all bootflash:
    -#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
    1   .. unknown  FD38E5C7  3FD81C   25  3921820 Oct 02 1998 14:43:56 rsp-boot-mz.112-15a.P.bin
    2   .D config   AF12EF9F  41C308    9   125547 Oct 16 1998 11:10:10 crashinfo
    3   .D config   33DEAF65  43A950    9   124360 Oct 16 1998 11:15:50 crashinfo

    3430064 bytes available (4172112 bytes used)

Router# undelete 2 bootflash:
    Router#dir /all bootflash:
    -#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
    1   .. unknown  FD38E5C7  3FD81C   25  3921820 Oct 02 1998 14:43:56 rsp-boot-mz.112-15a.P.bin
    2   .. config   AF12EF9F  41C308    9   125547 Oct 16 1998 11:10:10 crashinfo
    3   .D config   33DEAF65  43A950    9   124360 Oct 16 1998 11:15:50 crashinfo

    3430064 bytes available (4172112 bytes used)
```

Monitoring and Maintaining the Cisco 12000 Series Internet Router

There are a number of **show** commands that can be used to monitor the Cisco 12000 Series Internet Router as it runs. A subset of the most useful of these commands is described here. For a complete discussion of all available **show** commands, refer to the *Cisco IOS Command Reference*.

- Monitoring the Router Configuration, page 3-11
- Additional System Monitoring, page 3-14
- Monitoring and Maintaining the PRP Software Configuration, page 3-15

Monitoring the Router Configuration

To monitor the router interface configuration, use the following **show** commands in EXEC mode:

Command	Purpose
Router# **show version**	Displays the Cisco IOS software version number, hardware installed in the router, the names and sources of the router image files, and the contents of the software configuration register.
Router> **show gsr**	Displays the statistics of each hardware module installed in the Cisco 12000 Series Internet Router.
Router> **show interfaces**	Displays information about the system interfaces.
Router> **show interfaces** *type slot/port*	Displays information about a specific interface in the system. *Type* indicates the interface type, for example, pos, srp, atm; *slot/port* indicates the interface location in the router.
Router> **show diags** *slot*	Displays specific hardware information for the card installed in the specified slot in your system, including the card serial number.
Router> **show running-config**	Displays the currently running configuration in RAM.
Router> **show led**	Displays the current LED status on all line cards.
Router> **show ip interface** [**brief**]	Displays the usability status of interfaces configured for IP.

The following sample display shows typical results from the **show version** command. Depending on the image version of the Cisco IOS software running on your router and the way the router is equipped, the results of your **show version** command might be different.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M), Experimental Version 12.0(20020822:053101) [ozarad-offLci
151]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 26-Aug-02 14:20 by ozarad
Image text-base: 0x50010968, data-base: 0x52C44000

ROM: System Bootstrap, Version 11.2(20010625:183716) [bfr_112 181], DEVELOPMENT SOFTWARE
BOOTLDR: GS Software (GSR-BOOT-M), Version 12.0(8)S, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)

Q311 uptime is 1 day, 3 hours, 15 minutes
System returned to ROM by reload at 11:52:01 UTC Sun Aug 4 2002
System restarted at 11:28:14 UTC Sat Aug 10 2002
System image file is "tftp://172.16.16.254/gsr-p-mz.ME12_SRP_VER_13_08_28_02"

cisco 12406/GRP (R5000) processor (revision 0x05) with 131072K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on

1 Route Processor Card
2 Clock Scheduler Cards
3 Switch Fabric Cards
2 one-port OC48 SONET based SRP controllers (2 SRP).
1 OC12 POS controller (1 POS).
1 OC48 POS controller (1 POS).
1 two-port OC12 SONET based SRP Edge based controller (2 SRP).
1 Ethernet/IEEE 802.3 interface(s)
2 Packet over SONET network interface(s)
3 SRP network interface(s)
507K bytes of non-volatile configuration memory.

8192K bytes of Flash internal SIMM (Sector size 256K).
```

```
Configuration register is 0x2102
```

The following sample display shows typical results from the **show gsr** command. For each hardware module installed in the chassis, the state string describes its status. The state string generally corresponds to the value displayed on the alphanumeric LEDs on the hardware module, as shown in Table 3-6.

```
Router> show gsr
Slot 0  type  = 2 Ports OC3 Channelized to DS1/E1
        state = IOS RUN   Line Card Enabled
Slot 1  type  = 3 Port Gigabit Ethernet
        state = IOS RUN   Line Card Enabled
Slot 5  type  = Route Processor
        state = ACTV RP   IOS Running  ACTIVE
Slot 17 type  = Clock Scheduler Card(6) OC-192
        state = Card Powered  PRIMARY CLOCK
Slot 18 type  = Switch Fabric Card(6) OC-192
        state = Card Powered
Slot 19 type  = Switch Fabric Card(6) OC-192
        state = Card Powered
Slot 20 type  = Switch Fabric Card(6) OC-192
        state = Card Powered
Slot 24 type  = Alarm Module(6)
        state = Card Powered
Slot 25 type  = Alarm Module(6)
        state = Card Powered
Slot 28 type  = Blower Module(6)
        state = Card Powered
```

Table 3-6 Alphanumeric LED Display vs. show gsr State String

Alphanumeric LED Display	show gsr State String
none	ABSENT Card absent
ACTV STRT	ACTVSTRT Active RP startup
ACTV RP	ACTV RP IOS Running ACTIVE
ADMN DOWN	ADMNDOWN Administratively down
ADMN OFF	ADMNOFF Administratively powered down
BWTH LOW	BWTHLOW Bring up suspended low bandwidth condition
CARV ERR	CARVERR Bring up suspended buffer carving error
DIAG F LD	DIAGF LD Downloading field diagnostics over fabric
DIAG HALT	DIAGHALT Cancel field diagnostics
DIAG LOAD	DIAGLOAD Downloading field diagnostics over MBus
DIAG PASS	DIAGPASS Field diagnostics ran successfully
DIAG STRT	DIAGSTRT Launching field diagnostics
DIAG TEST	DIAGTEST Running field diagnostic tests
DUMP DONE	DUMPDONE Completed data collection after failure
DUMP REQ	DUMPREQ Line Card or RP requesting core dump
DUMP RUN	DUMPRUN Line Card or RP core dumping
FABI WAIT	FABIWAIT Waiting for fabric inititialization to be complete for card
FABL DNLD	FABLDNLD Loading fabric downloader
FABL RUN	FABLRUN Fabric downloader ready for use

Table 3-6 Alphanumeric LED Display vs. show gsr State String

Alphanumeric LED Display	show gsr State String
FABL STRT	FABLSTRT Launching fabric downloader
FABM WAIT	FABMWAIT Wait for fabric manager to report fabric usable
IN RSET	IN RSET In reset
IOS DNLD	IOSDNLD Downloading IOS
IOS FABW	IOSFABW IOS in startup waiting for fabric to be ready
IOS VGET	IOSVGET Getting IOS version number
IOS RUN	IOS RUN Line card enabled
IOS STRT	IOS STRT Starting IOS
IOS TRAN	IOS TRAN Transitioning to active
IOS UP	IOS UP IOS is running
MAL FUNC	MAL FUNC Card malfunction reported by field diagnostics
MISM ATCH	MISMATCH Card type mismatch with card in paired slot
none	POWERED Card powered
CYC	PWR CYC Card undergoing a power cycle
OFF	PWR OFF Card NOT powered
PWR STRT	PWR STRT Card newly powered
ROMI GET	ROMIGET Getting ROM images
ROM VGET	ROMVGET Getting ROM response
OFF	RP OFF Route processor not powered
RP RDY	RP RDY Route processor powered
WAIT	RTRYWAIT Waiting to retry download after persistent failures
SCFG PRES	SCFGPRES Incorrect "hw-module slot # srp" command present
SCFG REQD	SCFGREQD Required "hw-module slot # srp" command not present
STBY STRT	STBYSTRT Launching IOS (Standby)
STBY RP	STBY RP IOS Running STANDBY
none	UNKNSTAT Unknown
XS RP	XS RP GRP/PRP not required in chassis

Additional System Monitoring

The following additional commands can be used to monitor various system indicators:

Command	Purpose
`Router# show controllers`	Displays information about the hardware. There is a **show controllers** command for the RP and a separate **show controllers** command for line cards.
`Router# show context`	Displays information stored in NVRAM when the router crashes. This command is only useful to technical support representatives.

Command	Purpose
Router# **show environment**	Displays the current environmental specifications.
Router# **show logging**	Displays the state of the syslog error and event logging. Before using this command, you should configure the system to timestamp logging messages with the **service timestamps** command. To clear messages from the logging buffer, use the **clear logging** command.
Router# **show memory**	Displays memory pool statistics, including summary information about the activities of the system memory allocator and a block-by-block listing of memory use.
Router# **show microcode**	Displays the microcode bundled into the system image.
Router# **show processes**	Displays information about all active processes.
Router# **show protocols**	Displays the configured protocols.
Router# **show stacks**	Displays stack usage of processes and interrupt routines, including the reason for the last system reboot. This command is only useful to your technical support representative.
Router# **show tcp**	Displays the status of TCP connections.
Router# **show tcp brief** [**all**]	Displays a concise description of TCP connection endpoints.
Router# **show tech-support** [**page**] [**password**]	Displays general information about the router when reporting a problem.

Monitoring and Maintaining the PRP Software Configuration

To monitor the configuration of the PRP, use the following **show** commands in EXEC mode:

Command	Purpose
Router# **show controllers ethernet**	Displays the register values and status of the GT64260 Ethernet controllers.
Router# **show controllers gt64260**	Displays the register values of the GT64260 Discover System controller.
Router# **show controllers psar**	Displays statistics about the packets sent and received in the PRP packet segmentation and reassembly (PSAR) controllers.

CHAPTER 4

Command Reference

This chapter describes Cisco 12000 Series Internet Router commands that are not described in the Cisco IOS Command Reference for Release 12.0S or in any Cisco IOS Feature Module document. It describes the following commands:

arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** global configuration command. To remove an entry from the ARP cache, use the **no** form of this command.

arp [**vrf** *vrf-name*] *ip-address hardware-address type* [{**alias** | *interface*}]

no arp [**vrf** *vrf-name*] *ip-address*

Syntax Description

vrf	Configures static ARP entries for an individual Virtual Private Network (VPN) routing and forwarding table (VRF).
vrf-name	VPN routing and forwarding table name.
ip-address	IP address of the ARP entry.
hardware-address	48-bit hardware address of the ARP entry, in the format H.H.H.
type	Encapsulation description. For Ethernet interfaces, this is typically the **arpa** keyword. For Fiber Distributed Data Interface (FDDI) and Token Ring interfaces, this is always **snap**. Other possibilities are **sap** (HP's ARP type), **smds**, and **srp-a** or **srp-b**.
alias	(Optional) Indicates that the Cisco IOS software should respond to ARP requests as if it were the owner of the specified address.
interface	(Optional) Interface identifier.

Defaults

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced
12.0(22)S	This command was changed to include configuring static ARP entries per VRF.

Usage Guidelines

The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally do not need to specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
Router# arp 192.168.7.19 0800.0900.1834 arpa
```

The following is an example of an ARP for a VRF:

```
Router(config)# arp vrf v4 20.1.1.1 0000.0000.0001 arpa
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.

clear psar

To reset and restart all packet statistics maintained in the PRP segmentation and reassembly (PSAR) drivers, use the **clear psar** command in global configuration mode.

clear psar

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The **clear psar** command replaces the **clear csar** command used on the Gigabit Route Processor.

Examples

The following example shows how to clear all statistics recorded in the PSAR drivers:

```
Router# clear psar
```

description

To enter comments about your Virtual Private Network (VPN) routing and forwarding (VRF) configuration, use the **description** VRF submode command.

description *text*

Syntax Description

text	Up to 80 characters of text describing this VRF.

Defaults

No default behavior or values.

Command Modes

VRF submode

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

Use this command to provide descriptive text about a particular VRF.

Examples

The following is an example of the VRF **description** command:

```
Router(config-vrf)# description This is my 4th VRF
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
show ip vrf	Displays information about a VRF or all VRFs.

diag

To perform field diagnostics on a line card, Route Processor card (RP), including both the Performance Route Processor (PRP) and Gigabit Route Processor (GRP), Switch Fabric Card (SFC), or Clock Scheduler Card (CSC) in Cisco 12000 Series Internet Routers, use the **diag** command in privileged EXEC configuration mode. To halt a running field diagnostic session on a line card or RP, use the **diag halt** form of this command.

Cisco 12000 Series Internet Router line cards

diag *slot-number* [**mbus**] [**verbose**] [**wait**] [**full**] [**coe**] **source** {**tftp** | **flash**} *source_path*

diag *slot-number* **previous**

diag *slot-number* **halt**

Cisco 12000 Series Internet Router RPs

diag *slot-number* [**verbose**] [**wait**] [**full**] [**coe**]

diag *slot-number* **previous**

diag *slot-number* **halt**

Cisco 12008, Cisco 12012, and Cisco 12016 SFCs and CSCs

diag *slot-number* [**verbose**]

Syntax Description

slot-number	Slot number of the card you want to test.
source	Specifies the source path of the line card diagnostic image. The name of the image file is **c12k-fdiagsbflc.***120-22.2.S*, where 120-22.2.S is the version number. For Flash cards, the source path would typically be **slot0:c12k-fdiagsbflc.***120-22.2.S* or **slot1:c12k-fdiagsbflc.***120-22.2.S*. The TFTP source path would typically be **tftp://***tftp_server_ip_address/my_directory***/c12k-fdiagsbflc.***120-22.2.S*. This option is available and required for line card testing only. This keyword must be followed by either the **tftp** or **flash** keyword.
halt	(Optional) Stops the field diagnostic testing on the line card. This option is only available for line cards and RPs.
previous	(Optional) Displays previous test results (if any) for the card. This option is only available for line cards and RPs.
verbose	(Optional) Enables progress and error messages to be displayed on the console. By default, only the minimum status messages are displayed on the console, along with the final result. Due to the comprehensive nature of testing, testing without the verbose option will result in up to a 15-minute delay before any results are displayed. Cisco recommends that the verbose option be specified and results captured when communicating with Cisco TAC.

wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the successful completion of the field diagnostic testing. If you use this keyword, you must use the **microcode reload slot** global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the RP recognizes the line card and downloads the Cisco IOS software image to the line card.
mbus	(Optional) Forces the download to use the MBus as the path to download the line card diagnostic image. Normally the switch fabric is used to move the image to the line card to be tested. This takes only a few seconds, but requires much of the line card to be functional. The MBus download can take more than 15 minutes to download, but requires very little of the line card to be functional. For testing the standby RP, only MBus download can be used, and this is the default mode. SFCs and CSCs are not tested with a downloaded image.
coe	(Optional) Continue On Error. Normally the field diagnostics stop immediately upon failing any one test within a test session. Using the **coe** keyword forces the testing to continue to the end of the internal test list, even if a failure occurs. Caution should be exercised because in some cases where a cascade of failures is found, using this option MAY require the router to be reloaded, affecting all RPs and line cards. This option is only available for line cards and RPs.
full	(Optional) The default set of tests emphasize memory and data path tests. To force the line card or RP to complete the most extensive set of tests, use the full option. The test time will be slightly longer. This option is only available for line cards and RPs.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was added to support the Cisco 12000 Series Internet Routers.
12.0(22)S	The **source** option was added for line cards.

Usage Guidelines

Before you can use the line card field diagnostics commands, you must place a valid diagnostics image on a separate Flash memory card installed in the Cisco 12000 Series Internet Router to be tested or on a TFTP boot server. The diagnostics image is named **c12k-fdiagsbflc-mz.***120-22.S* (where 120-22.S is the version number) and is always available on Cisco.com.

RP, SFC, and CSC field diagnostics are embedded within the IOS image and thus do not require an external image.

The following Engine 0 line cards include components that are unable to isolate internal line card testing traffic from customer premise connections:

- 4-port OC-3/STM-1c POS
- 1-port OC-12/STM-4c POS

- 4-port OC-3/STM-1c ATM
- 1-port OC-12c/STM-4c ATM

When testing these line cards, you are warned and notified to disconnect any connections to these line cards before testing to achieve the most reliable results and minimize traffic disruption.

The diagnostics software prompts you for confirmation before altering the router configuration. For example, running diagnostics on an SFC or CSC will cause the fabric to go from full bandwidth to one-quarter bandwidth. Bandwidth is not affected by RP or line card diagnostics.

Perform diagnostics on the CSC only if a redundant CSC is in the router. Diagnostics can be performed on redundant RPs only. Currently SFC and CSC testing is not available for Cisco 12400 Series Internet Routers.

Note No cyclic redundancy check (CRC) error is reported in Cisco IOS software when a CRC error occurs on the Cisco 12010, 12410, or 12810 Internet Router. As a result, the faulty switch fabric card (SFC) is not shut down.

This problem has been resolved in IOS Release 12.0(26)S and later releases. However, in IOS Release 12.0(24)S or 12.0(25)S, if you suspect a switch fabric failure, you must use the **show controllers fia** command to display information about the Fabric Interface ASIC (FIA) controllers on the router. The FIA resides on both the Route Processor (RP) and line cards (LCs). It provides an interface between the RP/LC and the switch fabric cards.

As described in *Hardware Troubleshooting for the Cisco 12000 Series Internet Router*, enter the **show controllers fia** on the RP and on individual line cards to troubleshoot. Then take one of the following actions:

- If the results displayed by the **show controllers fia** command for line cards and the RP show CRC errors on the same SFC, verify that the card is correctly seated and then, if necessary, shut down and replace the SFC.

- If the results displayed by the **show controllers fia** command show that an SFC is faulty only on one line card, replace and then reload the line card.

- If the results displayed by the **show controllers fia** command show that more than one SFC is faulty on multiple line cards, replace primary clock and scheduler card (CSC).

For detailed information about the **show** command output, refer to *How To Read the Output of the Show Controller fia Command.*

Caution Performing field diagnostics on a line card stops all activity on the line card. Before the **diag** command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

In normal mode, if a test fails, the title of the failed test is displayed on the console. However, not all tests that are performed are displayed. To view all performed tests, use the **verbose** keyword.

After all diagnostic tests are completed on the line card, a PASSED or TEST FAILURE message is displayed. If the line card sends a PASSED message, the Cisco IOS software image on the line card is automatically reloaded unless the **wait** keyword is specified. If the line card sends a TEST FAILURE message, the Cisco IOS software image on the line card is not automatically reloaded.

If you want to reload the line card after it fails diagnostic testing, use the microcode **reload slot** global configuration command.

Note When you stop the field diagnostic test using the **diag halt** command, the line card remains down (that is, in an unbooted state). Generally, you would stop testing in order to remove or replace the line card. If this is not the case, and you need to bring the line card back up (online), use the microcode **reload** global configuration command or power cycle the line card.

If the line card fails the test, the line card is defective and should be replaced. Under certain circumstances, TAC engineers may direct you to replace field-replaceable memory modules and retest. This should ONLY be done under the guidance of a TAC engineer. For example, if the DRAM test failed, a customer might only need to replace the DRAM on the line card.

For more information, refer to the appropriate Cisco 12000 Series Internet Router installation and configuration guide.

Examples

The following example shows the output when field diagnostics are performed on the line card in slot 7. After the line card passes all field diagnostic tests, the Cisco IOS software is automatically reloaded on the card. Before starting the diagnostic tests, you must confirm the request to perform these tests on the line card because all activity on the line card is halted. The message “total/indiv. timeout set to 2000/600 sec.” indicates that 2000 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 600 seconds to complete.

```
Router# diag 7 source tftp tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-22.S
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus' option.
Runnning Diags will halt ALL activity on the requested slot.  [confirm]
award-rp-slot0#
Launching a Field Diagnostic for slot 7
Downloading diagnostic tests to slot 7 via fabric (timeout set to 300 sec.)
5d20h: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event: EV_ADMIN_FDIAG
Loading images/award/c12k-fdiagsbflc-mz.120-22.S from 192.164.1.1 (via Ethernet0):
!!!!!
5d20h: Downloading diags from tftp file
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-22.S
!!!!![OK - 13976524 bytes]
FD 7> *****************************************************
FD 7> GSR Field Diagnostics V6.05
FD 7> Compiled by award on Tue Jul 30 13:00:41 PDT 2002
FD 7> view: award-conn_isp.FieldDiagRelease
FD 7> *****************************************************
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 7> BFR_CARD_TYPE_OC12_4P_POS testing...
FD 7> Available test types 2
FD 7>                      1
FD 7> Completed f_diags_board_discovery() (0x1)
FD 7> Test list selection received: Test ID 1, Device 0
FD 7> running in slot 7 (30 tests from test list ID 1)
FD 7> Skipping MBUS_FDIAG command from slot 2
FD 7> Just into idle state
Field Diagnostic ****PASSED**** for slot 7
Shutting down diags in slot 7
Board will reload
5d20h: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event: EV_ADMIN_FDIAG
SLOT 7:00:00:09: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
```

```
IOS (tm) GS Software (GLC1-LC-M), Experimental Version 12.0(20020509:045149)
[award-conn_isp.f_diag_new 337]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 25-Jun-02 15:51 by award
```

The following example shows the output of a line card test with the **verbose** option specified (highly recommended).

```
Router# diag 7 verbose tftp tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-22.S
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus' option.
Verbose mode: Test progress and errors will be displayed
Runnning Diags will halt ALL activity on the requested slot.  [confirm]
Router#
Launching a Field Diagnostic for slot 7
Downloading diagnostic tests to slot 7 via fabric (timeout set to 300 sec.)
00:07:41: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event: EV_ADMIN_FDIAG
Loading images/award/c12k-fdiagsbflc-mz.120-22.S from 192.164.1.1 (via Ethernet0):
!!!!!! (...)
00:08:24: Downloading diags from tftp file
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120.22.S
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13976524 bytes]
FD 7> ******************************************************
FD 7> GSR Field Diagnostics V6.05
FD 7> Compiled by award on Tue Jul 30 13:00:41 PDT 2002
FD 7> view: award-conn_isp.FieldDiagRelease
FD 7> ******************************************************
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 7> BFR_CARD_TYPE_OC12_4P_POS testing...
FD 7> Available test types 2
FD 7>                      1
FD 7> Completed f_diags_board_discovery() (0x1)
FD 7> Verbosity now (0x00000011) TESTSDISP FATL
FD 7> Test list selection received: Test ID 1, Device 0
FD 7> running in slot 7 (30 tests from test list ID 1)
FD 7> Just into idle state
FDIAG_STAT_IN_PROGRESS(7): test #1 Dram Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #2 Dram Datapins
FDIAG_STAT_IN_PROGRESS(7): test #3 Dram Busfloat
FDIAG_STAT_IN_PROGRESS(7): test #4 RBM SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #5 RBM SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #6 RBM SSRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #7 RBM SSRAM Datapins Memory
FDIAG_STAT_IN_PROGRESS(7): test #8 TBM SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #9 TBM SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #10 TBM SSRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #11 TBM SSRAM Datapins Memory
FDIAG_STAT_IN_PROGRESS(7): test #12 PSA TLU SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #13 PSA TLU SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #14 PSA PLU SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #15 PSA PLU SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #16 PSA SRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #17 PSA SRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #18 To Fabric SOP FIFO SRAM Memory
FDIAG_STAT_IN_PROGRESS(7): test #19 From Fabric SOP FIFO SRAM Memory
FDIAG_STAT_IN_PROGRESS(7): test #20 RBM to SALSA Packet
FDIAG_STAT_IN_PROGRESS(7): test #21 TBM to SALSA Packet
FDIAG_STAT_IN_PROGRESS(7): test #22 RBM to TBM SLI Packet Loopback
FDIAG_STAT_IN_PROGRESS(7): test #23 TBM to PSA Packet - Framer Loopback
FDIAG_STAT_IN_PROGRESS(7): test #24 TBM to TX SOP Packet
FDIAG_STAT_IN_PROGRESS(7): test #25 TBM to RX SOP Packet - 4302 Terminal Loopback
FDIAG_STAT_IN_PROGRESS(7): test #26 TBM to RX SOP Packet - Framer System Bus Loop
FDIAG_STAT_IN_PROGRESS(7): test #27 RBM to TBM Fabric Packet Loopback
FDIAG_STAT_IN_PROGRESS(7): test #28 TBM to RBM Packet, RBM page crossing
FDIAG_STAT_IN_PROGRESS(7): test #29 TBM to TX SOP Packet Simultaneous
FDIAG_STAT_IN_PROGRESS(7): test #30 TBM to PSA Multicast Packets - Framer Loopbac
FDIAG_STAT_DONE(7)
FD 7> Changed current_status to FDIAG_STAT_IDLE
Field Diagnostic ****PASSED**** for slot 7
Field Diag eeprom values: run 62 fail mode 0 (PASS) slot 7
last test failed was 0, error code 0
Shutting down diags in slot 7
Board will reload
```

Following is an example of a test FAILURE condition on a GRP card. This card would need to be replaced and returned to Cisco for repair:

```
Field Diag download COMPLETE for slot 3
FD 3> *****************************************************
FD 3> GSR Field Diagnostics V6.01
FD 3> Compiled by award on Tue Apr 9 07:22:53 PDT 2002
FD 3> view: award-conn_isp.f_diag_new
FD 3> *****************************************************
Diagnostics have been downloaded to slot 3
Executing all diagnostic tests in slot 3
(total/indiv. timeout set to 2000/600 sec.)
FD 3> BFRP w/ECC testing...
FD 3> Secondary Discovery found ID 2
FD 3> BFR_CARD_TYPE_BFRP_CARD w/ ECC testing...
FD 3> Available test types 2
FD 3>                      1
FD 3> Completed f_diags_board_discovery() (0x1)
FD 3> Verbosity now (0x00000011) TESTSDISP FATL
FD 3> Test list selection received: Test ID 1, Device 0
FD 3> running in slot 3 (24 tests from test list ID 1)
FDIAG_STAT_IN_PROGRESS(3): test #1 BFRP Dram Datapins Test
FDIAG_STAT_IN_PROGRESS(3): test #2 Dram Marching Pattern Test
FDIAG_STAT_IN_PROGRESS(3): test #3 DataPins_Sram
FDIAG_STAT_IN_PROGRESS(3): test #4 March_Sram
FDIAG_STAT_IN_PROGRESS(3): test #5 High Memory DRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(3): test #6 diags_csar_regtest
FDIAG_STAT_IN_PROGRESS(3): test #7 diags_test_p4_csar_int
FDIAG_STAT_IN_PROGRESS(3): test #8 NVRAM Memory Test
FD 3> 32 bit data compare error. Wrote 0xcccccccc, read back 0xcc41cccc at location
0xbe03fff0
FDIAG_STAT_DONE_FAIL(3) test_num 8, error_code 1
COMPLETED Field Diags: pid 128, status 5, test_num 8, error_code 1
Field Diagnostic: ****TEST FAILURE**** slot 3: first test failed: 8,
NVRAM Memory Test, error 1
Field Diag results from eeprom before updating slot 3, run# 0x5000042 were 0x0
previous field diag eeprom values: run 66 fail mode 5 (DOWNLOAD FAILURE)
last test failed was 0, error code 0
Field Diag eeprom values: run 67 fail mode 1 (TEST FAILURE) slot 3
last test failed was 8, error code 1
Shutting down diags in slot 3
slot 3 done, will not reload automatically
```

The following example shows the previous test results of a line card. Diagnostics had been run 64 times on this line card. Because the board PASSED the last field diagnostics session, the fail mode was 0, as was the last test that failed.

```
Router # diag 7 prev
Field Diag eeprom values: run 64 fail mode 0 (PASS) slot 7
   last test failed was 0, error code 0
```

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card on the Cisco 12000 Series Internet Routers after all microcode configuration commands have been entered.

exception linecard crashinfo

To configure a Cisco 12000 Series Internet Router to save system crash information files in a location other than in the RP bootflash memory, use the **exception linecard crashinfo** command in global configuration mode. To specify that crash information data not be saved, use the **no** form of this command.

exception linecard {**slot** *slot-number* | **all**} **crashinfo file** *file-name*

no exception linecard {slot *slot-number* | **all**} **crashinfo**

Syntax Description

slot *slot-number*	Slot number of the line card for which you want configure the crashinfo file.
all	Configure the crashinfo file for all line cards in the chassis.

Defaults

By default the crashinfo file is saved to the RP bootflash.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.

Usage Guidelines

Line cards can generate a full crashinfo file that can be saved in nonvolatile storage. This is in addition to the mini-crashinfo that is saved in the RP RAM and can be viewed using the **show context** command.

By default, the line card crashinfo file is saved to the RP bootflash, with the name crashinfo_yyyymmdd-hhmmss.x where x is the slot number. For example, a crashinfo file from a line card in slot 3 would appear as follows:

```
16  -rw-      175232   Jan 15 2003 20:00:25 crashinfo_20030115-200025.3
```

Line card crashinfo files are only saved to the bootflash if there is a reasonable amount of spare space in the bootflash. The design intent is to reserve sufficient space for RP crashinfo files, even if there are multiple linecard failures.

The **no** form of the command disables the saving of the line card crashinfo data.

Use the **exception linecard crashinfo** command to specify a filename when the line card crashinfo data is to be saved in an alternative location.

exception warmstart

To configure a Cisco 12000 Series Internet Router for a warmstart in case of a system crash, use the **exception warmstart** command in global configuration mode. To remove the warmstart configuration settings, use the **no** form of this command.

exception warmstart *min-uptime max-restarts* **[d]**

no exception warmstart *min-uptime max-restarts*

Syntax Description

min-uptime	Minimum amount of PRP uptime (in seconds) required before a warmstart is performed. Valid values are from 0 to 1000000.
max-restarts	Maximum number of IOS warmstarts allowed before a warmstart is no longer performed. Valid values are from 0 to 1000000.
d	Optional. Enables a warmstart if a second (dual) Performance Router Processor (PRP) is installed.

Defaults

The default for the minimum uptime is 60 seconds.

The default for the maximum number of restarts allowed is 5.

The warmstart feature defaults are as follows:

- Enabled if only one PRP is installed.
- Disabled if a second, standby PRP is installed in the router.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The warmstart feature allows the PRP in a Cisco 12000 Series Internet Router to restart the IOS software configuration after a crash, without having to reload the image from an external device.

Note As with other **exception** commands, use the **exception warmstart** command only as instructed and when asked to do so by Cisco technical support personnel.

If the PRP has been running for at least the amount of time specified by *min-uptime*, and if the system has not been restarted more than the number of times specified by *max-restarts,* the route processor restarts the Cisco IOS following a system crash.

In a dual PRP configuration (that is, when a redundant PRP is installed in the router), the warmstart feature is disabled by default. For this reason, you must specify **d** (for **d**ual) when you enter the **exception warmstart** command to enable a warmstart.

This feature does not affect the behavior of the **reload** command. Also, you can still perform a “send break” as usual from the console by pressing **Ctrl-Z**.

Examples

The following example applies to a redundant configuration in which two PRPs are installed. It shows how to configure a warmstart if the IOS software in the PRP has been running for at least 90 seconds, and if the system has not been restarted more than eight times:

```
Router# configure terminal
Router# exception warmstart 90 8 d
```

export map

To configure an export route map for a VRF, use the **export map** VRF submode command.

export map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an export route map for the VRF.

Defaults

There is no default. A VRF has no export route map unless one is configured using the **export map** command.

Command Modes

VRF submode

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

Use an export route map when an application requires finer control over the routes in a VRF than provided by the import and export extended communities configured for importing and exporting VRF.

Examples

The following example shows how to configure an export route map for a VRF:

```
Router(config)# ip vrf vrf_blue
Router(config-vrf)# export map blue_export_map
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
route-target	Configures import and export extended community attributes for the VRF.
show ip vrf	Displays information about a VRF or all VRFs.

hw-module reload

To reload a line card, use the **hw-module reload** privileged EXEC command.

hw-module slot *slot-number* **reload**

Syntax Description

slot *slot-number*	Slot number of the line card that you want to reload.

Defaults

There are no defaults.

Command Modes

Privileged EXEC

Usage Guidelines

This command causes the line card to reset and redownload the Maintenance Bus (MBus) and Fabric Downloader software modules before attempting to redownload the line card Cisco IOS software.

Examples

In the following example, the line card in slot 3 is reloaded.

```
Router# hw-module slot 3 reload
```

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card.

hw-module warm-reboot (Privileged EXEC)

To initiate a warm reboot of a line card, use the **hw-module warm-reboot** privileged EXEC command.

hw-module slot *slot-number* **warm-reboot**

Syntax Description

slot *slot-number*	Slot number of the line card that you want to reload.

Defaults

There are no defaults.

Command Modes

Privileged EXEC

Usage Guidelines

A warm reboot restarts the Cisco IOS image that is already installed on the line card. The effect is similar to a reload, except that the line card returns to service in a shorter amount of time.

If the line card is in a state where a warm reboot is not possible, then a full reload is performed.

A warm reboot does not reset any of the line card hardware.

Some line cards do not support a warm reboot. If you use this command on such a card, a reload is performed.

Examples

In the following example, the line card in slot 3 is warm rebooted.

```
Router# hw-module slot 3 warm-reboot
```

Related Commands

Command	Description
hw-module reload	Reloads the Cisco IOS image on a line card.

hw-module warm-reboot (Global Configuration)

To enable warm reboots of a line card, use the **hw-module warm-reboot** global configuration command. To disable warm reboots on a line card, use the **no** form of this command.

hw-module slot *slot-number* **warm-reboot**

no hw-module slot *slot-number* **warm-reboot**

Syntax Description

slot *slot-number*	Slot number of the line card that you want to reload.

Defaults

This command is enabled by default.

Command Modes

Global configuration

Usage Guidelines

This command enables or disables the use of warm reboot by the system to recover from possible line card problems. By default, warm reboot is enabled. If warm reboot is disabled using the **no** form of this command, line card failures will result in a full reload.

Having warm reboot enabled does not mean that the system will use this method of error recovery. The RP has a set of criteria for choosing the recovery method and will only use warm reboot in a limited set of instances.

If an automatic warm reboot fails, the system will peform a full reload of the card.

There may be specific line cards that do not support warm reboot. For these line cards, the warm reboot option is automatically disabled.

Examples

In the following example, the warm reboot on the line card in slot 3 is disabled.

```
Router(config)# no hw-module slot 3 warm-reboot
```

Related Commands

Command	Description
hw-module warm-reboot (Privileged EXEC)	Reloads the Cisco IOS image on a line card.

ip pim sparse-mode-register

To register directly connected sources, use the **ip pim sparse-mode-register** command in interface configuration mode. Use the **no** form of this command to stop registering directly connected sources.

ip pim sparse-mode-register

no pim sparse-mode-register

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default when PIM sparse-mode is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(18)S	This command was introduced.

Usage Guidelines

The **ip pim sparse-mode-register** command is available on Cisco 12000 Series Internet Routers Packet-over-SONET (POS) interfaces on Engine 4 line cards, and the command only applies when PIM sparse-mode (for multicast) is enabled. By default, this command is enabled and stored in NVRAM as the default, and the router will perform normally. If **no ip pim sparse-mode-register** is configured, the router will not register directly connected sources. This action only affects sparse-mode groups, not dense-mode groups or source-specific-mode groups.

It is recommended that you configure **no ip pim sparse-mode-register** to save memory in hardware-forwarding database of Engine 4 line cards if you do not have directly connected sources, such as typical backbone links.

ip route-cache flow

To enable NetFlow switching for IP routing, use the **ip route-cache flow** command in interface configuration mode. To disable NetFlow switching, use the **no** form of this command.

ip route-cache flow [**sampled** [**input** | **output**]]

no ip route-cache flow [**sampled** [**input** | **output**]]

Syntax Description

sampled	(Optional) Enables NetFlow cache in sampled mode.
input	(Default) Enables NetFlow sampling on inbound IP flows.
output	Enables NetFlow sampling on outbound flows

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(11)S	The **sampled** keyword was added.
12.0(22)S	The **input** and **output** keywords were added.

Usage Guidelines

NetFlow is an accounting and acceleration mechanism that captures a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type-of-service information that can be used for a wide variety of purposes, such as network analysis and planning, accounting, and billing. To export NetFlow data, use the **ip flow-export global** configuration command.

NetFlow is supported on IP and IP encapsulated traffic over all interface types and encapsulations except for Inter-Switch Link/VLAN, ATM, and Frame Relay interfaces when more than one input access control list is used on the interface, and ATM local area network emulation (LANE).

In conventional switching at the network layer, each incoming packet is handled on an individual basis with a series of functions to perform access list checks, capture accounting data, and switch the packet. With NetFlow, after a flow has been identified and access list processing of the first packet in the flow has been performed, all subsequent packets are handled on a “connection-oriented” basis as part of the flow, where access list checks are bypassed and statistics captures are performed in tandem.

A network flow is identified as a unidirectional stream of packets between a source and destination—both defined by a network-layer IP address and transport-layer port number. Specifically, a flow is identified as the combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number

- Protocol type
- Type of service
- Input interface

NetFlow operates by creating a flow cache that contains the information needed to perform access list check for all active flows. The NetFlow cache is built by processing the first packet of a flow through the standard fast switching path. As a result, each flow is associated with an incoming and outgoing interface port number and with a specific security access permission and encryption policy. The cache also includes entries for traffic statistics that are updated in tandem with the switching of subsequent packets. After the NetFlow cache is created, packets identified as belonging to an existing flow have their traffic statistic counters incremented and security access list checks bypassed. Flow information is maintained within the NetFlow cache for all active flows.

NetFlow is not one of the available switching modes. When you configure NetFlow on an interface, you must have some other switching method to actually switch the packet. Also, with NetFlow you can export data (traffic statistics) to a remote workstation for further processing.

NetFlow accounting is based on identifying packet flows and maintaining statistics and access list processing within a router. It does not involve any connection-setup protocol—either between routers or to any other networking device or end station—and does not require any change externally—either to the traffic or packets themselves or to any other networking device. Thus, NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Because NetFlow is performed independently on each internetworking device, it does not need to be operational on each router in the network. Network planners can selectively invoke NetFlow accounting (and NetFlow data export) on a router/interface basis to gain traffic performance, control, or accounting benefits in specific network locations.

Note When sampled NetFlow is disabled on an interface, normal NetFlow also becomes disabled. This restriction was made to prevent the interface from being overwhelmed by the sudden transition from sampled NetFlow to normal NetFlow. You need to explicitly reenable NetFlow if so desired. The default value for the sampling interval is four billion. This default packet interval was designed to protect the router from being choked by a misconfiguration. You need to explicitly configure a usable packet interval for your case.

Note NetFlow consumes additional memory and CPU resources in comparison with other switching modes; therefore, it is important to understand the resources required on your router before enabling NetFlow.

Note Full NetFlow does not work on Engine 2 line cards. Although you can complete the full configuration, only Sampled NetFlow will work.

Examples

The following example enables NetFlow switching on the interface:

```
interface ethernet 0/5/0
 ip address 17.252.245.2 255.255.255.0
 ip route-cache flow
```

Related Commands

Command	Description
ip flow-export	Enables the exporting of information in NetFlow cache entries.

ip verify unicast source reachable-via

To enable and configure Reverse Path Forwarding (RPF) checks, use the **ip verify unicast source reachable-via** command in interface configuration mode. Use the **no** form of this command to disable RPF.

ip verify unicast source reachable-via {**any** | **rx**} [**allow-default**] [**allow-self-ping**]

no ip verify unicast

Syntax Description

any	Checks that the source address is reachable on any path.
rx	Checks that the source address is reachable on the interface on which the packet was received.
allow-default	(Optional) Checks that the default route matches the source address.
allow-self-ping	(Optional) Allows the router to ping itself.

The optional *access-list*, **allow-self-ping**, **allow-default**, and **any** (enables loose checking mode) parameters, that are supported in the **ip verify unicast source reachable-via** command for IPv4 traffic on other platforms, are now supported for the **ipv6 verify unicast source reachable-via rx** command on the Cisco 12000 Series Internet Router with release 12.0(33)S.

Note The **allow-default** parameter is not supported in E3 and E5 line cards.

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	Support for this command was introduced to the Cisco 12000 Series Internet Router IP services engine (ISE) line cards.

Usage Guidelines

Unicast RPF provides three basic modes:

- Exists-only mode—A source address need only be present in theJForwarding Information Base (FIB) and reachable through a “real” interface; this situation also applies to the **ip verify unicast source reachable-via any allow-default** command. The exists-only mode requires that a resolved and reachable source address is present in the FIB table. The source address must be reachable through a configured interface.
- Any mode—The source must be reachable through any of the paths. For example, the source has per-destination load balancing.
- RX mode—A source address must be reachable on the arrived interface. For example, the source must be reachable without load balancing.

Note Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

To use Unicast RPF, enable Cisco Express Forwarding (CEF) switching or dCEF switching in the router. You do not need to configure the input interface for CEF switching. As long as CEF is running on the router, you can configure individual interfaces with other switching modes.

Note Unicast RPF will not work without CEF.

Do not use Unicast RPF on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, which means that there are multiple routes to the source of a packet. You should apply Unicast RPF only where there is natural or configured symmetry.

Examples

This example shows how to enable Unicast RPF exist-only checking mode:

```
Router(config-if)# ip verify unicast source reachable-via any
```

Related Commands

Command	Description
ip cef	Refer to Cisco IOS documentation

microcode (Cisco IOS image)

To specify which Cisco IOS software image to load on a line card at reload, use the **microcode** global configuration command. To load the microcode bundled with the RP system image, use the **no** form of this command.

microcode {**card-type** *card-type* | **slot** *slot-number*} {**flash** *file-id* | **tftp** file-path}

no microcode {**card-type** *card-type* | **slot** *slot-number*} {**flash** *file-id* | **tftp** file-path}

Syntax Description

card-type *card-type*	Identifier of line card type that you want to copy the software image to. The identifier is a hexadecimal number between 0x21 and 0x79. Type a question mark (?) after the **card-type** keyword to see a list of valid card types.
slot *slot-number*	Slot number of the line card that you want to copy the software image to.
flash	Loads the image from the Flash file system.
file-id	Specifies the device and filename of the image file to download. A colon (:) must separate the device and filename (for example, slot0:gsr-p-mz). Valid devices are as follows: • **bootflash**—Internal Flash memory. • **slot0**—First PCMCIA slot. • **slot1**—Second PCMCIA slot.
tftp *file-path*	Loads the image from a TFTP server. *file-path* indicates the path to the TFTP server followed by the name of the image file.

Defaults

The image is loaded from the RP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2GS	This command was modified to load the Cisco IOS software image onto a line card in the Cisco 12000 Series Internet Routers.

Usage Guidelines

You must be in configuration mode to enter this command. The software image specified by this command is used when the system is booted, a line card is inserted or removed, or the microcode reload global configuration command is issued.

Immediately after you enter the **microcode reload** command and press **Return**, the system reloads all microcode. Global configuration mode remains enabled. After the reloading is complete, enter the exit command to return to the EXEC system prompt.

In addition to the Cisco IOS image that resides on the RP, each line card on a Cisco 12000 Series Internet Router has a Cisco IOS image. When the router is reloaded, the specified Cisco IOS image is loaded onto the RP, and that image is automatically downloaded to all the line cards.

Normally, you want the same Cisco IOS image on the RP and all line cards. However, if you want to upgrade a line card with a new version of microcode for testing or to fix a defect, you might need to load a Cisco IOS image that is different from the one on the line card. Additionally, you might need to load a new image on the line card to work around a problem that is affecting only one of the line cards.

Examples

In the following example, the Cisco IOS software image in Flash disk slot 0: is downloaded to the line card in slot 10 and the line card is rebooted using this image.

```
Router(config)# microcode slot 10 flash slot0:fip.v141-7
Router(config)# microcode reload 10
Router(config)# exit
```

To verify that the correct version is loaded, use the **execute-on slot 10 show version** command.

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card.

show frame-relay pvc

To display statistics about permanent virtual circuits (PVCs) for Frame Relay interfaces, use the **show frame-relay pvc** command in privileged EXEC mode.

show frame-relay pvc [**interface** *interface*] [*dlci* **64-bit**]

Syntax Description

interface	(Optional) Indicates a specific interface for which PVC information will be displayed
interface	(Optional) Interface number containing the DLCIs for which you wish to display PVC information.
dlci	(Optional) A specific DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified.
64-bit	Displays the 64-bit counters for the DLCI.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to display statistics about virtual access interfaces used for PPP connections over Frame Relay.
12.0(3)XG	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
12.0(4)T	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
12.0(5)T	This command was modified to include information on the special voice queue that is created using the **queue** keyword of the **frame-relay voice bandwidth** command.
12.1(2)T	This command was modified to include information about the policy map attached to a specified PVC.
12.0(17)S	This command was modified to include the 64-bit keyword and include information about 64-bit counters.

Usage Guidelines

Use this command to monitor the PPP link control protocol (LCP) state as being open with an “up” state, or closed with a “down” state.

When “vofr” or “vofr cisco” has been configured on the PVC, and a voice bandwidth has been allocated to the class associated with this PVC, configured voice bandwidth and used voice bandwidth are also displayed.

Statistics Reporting

To obtain statistics about PVCs on all Frame Relay interfaces, use this command with no arguments.

To obtain statistics about a PVC that include policy-map configuration, use this command with the DLCI argument.

Per-VC counters are not incremented at all when either autonomous or silicon switching engine (SSE) switching is configured; therefore, PVC values will be inaccurate if either switching method is used.

Traffic Shaping

Congestion control mechanisms are currently not supported, but the switch passes forward explicit congestion notification (FECN) bits, backward explicit congestion notification (BECN) bits, and discard eligible (DE) bits unchanged from entry to exit points in the network.

If a Local Management Interface (LMI) status report indicates that a PVC is not active, it is marked as inactive. A PVC is marked as deleted if it is not listed in a periodic LMI status message.

Examples

For detailed examples and explanations of displayed fields, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dtfrpqfq.htm#xtocid26

Related Commands

Command	Description
frame-relay pvc	Configures Frame Relay PVCs for FRF.8 Frame Relay-ATM Service Interworking.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.
show interfaces serial	Displays information about a serial interface.
show policy-map interface	Displays the configuration of classes configured for service policies on the specified interface or PVC.
show traffic-shape queue	Displays information about the elements queued at a particular time at the VC (DLCI) level.

show ip bgp dampening

To display BGP dampened routes, use the **show ip bgp dampening** EXEC command.

show ip bgp dampening dampened-paths

show ip bgp dampening flap-statistics [**regexp** *regexp* | **quote-exp** *quoteexp* | **filter-list** *access-list* | **cidr-only** | ip-*address mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*len*]]]

show ip bgp dampening parameters

Syntax Description

dampened-paths	Displays BGP dampened routes.
flap-statistics	Displays BGP flap statistics.
regexp *regexp*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-exp *quoteexp*	(Optional) Displays flap statistics for all the paths that match the regular expression contained within double quotes.
filter-list *access-list*	(Optional) Displays flap statistics for all the paths that pass the access list.
cidr-only	Displays flap statistics only for paths with non-natural netmasks.
ip-address	(Optional) Displays flap statistics for a single entry at this IP address.
mask	(Optional) Network mask applied to the value.
longer-prefixes	(Optional) Displays route and more specific routes.
injected	(Optional) Displays more specifics injected due to this prefix.
shorter-prefixes	(Optional) Displays less specific routes.
len	(Optional) Display prefixes longer than this mask length.
parameters	Displays details of the configured dampening parameters.

Defaults

There are no defaults.

Command Modes

EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.

Usage Guidelines

This command replaces the two commands **show ip bgp dampened-paths** and **show ip bgp flap-statistics**. It also adds the functionality of the **parameters** keyword.

Examples

The following is sample output from the **show ip bgp dampened-paths** command in privileged EXEC mode:

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse   Path
*d 10.0.0.0         171.69.232.177   00:18:4 100 ?
*d 12.0.0.0         171.69.232.177   00:28:5 100 ?
```

Table 4-1 describes the significant fields shown in the display.

Table 4-1 show ip bgp dampening dampened-paths

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

The following is sample output from the **show ip bgp flap-statistics** command in privileged EXEC mode:

```
Router# show ip bgp flap-statistics
BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 10.0.0.0         171.69.232.177  4     00:13:31 00:18:10 100
*d 12.0.0.0         171.69.232.177  4     00:02:45 00:28:20 100
```

Table 4-2 describes the significant fields shown in the display.

Table 4-2 show ip bgp dampening flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.

Table 4-2 show ip bgp dampening flap-statistics Field Descriptions (continued)

Field	Description
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

The following is sample output for the **show ip bgp dampening parameters** command:

```
Router# show ip bgp dampening parameters
dampening 10 1590 3000 30
Half-life time : 10 mins Decay Time : 1250 secs
Max suppress penalty: 12720 Max suppress time: 30 mins
Suppress penalty : 3000 Reuse penalty : 1590
```

Table 4-3 describes the significant fields.

Table 4-3 show ip bgp dampening parameters Field Descriptions

Field	Description
Half-life time	Configured value of half-life time (in minutes).
Decay time	Time (in seconds) for the penalty value to decay from maximum suppress penalty to suppress penalty. **Note** This value should not be too low.
Suppress penalty	Configured value of suppress penalty. A route is suppressed when its penalty exceeds this limit. The range is 1 to 20000; the default is 2000.
Reuse penalty	Configured value of reuse penalty. If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is 1 to 20000; the default is 750.
Max suppress time	Configured value of maximum suppress time (the maximum time, in minutes, that a route can be suppressed). The range is 1 to 20000; the default is 4 times the half-life. If the half-life value is allowed to default, the maximum suppress time defaults to 60 minutes.
Max suppress penalty	Calculated based on reuse penalty and maximum suppress time. When a route is penalized, its penalty value increases. The penalty cannot increase more than the maximum suppress penalty.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route-dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.
clear ip bgp dampening	Clears BGP route-dampening information and unsuppresses the suppressed routes.

show led

To display the current status of all line card Light Emitting Diodes (LEDs), use the **show led** EXEC command.

show led [*slot-number*]

Syntax Description

slot-number	Slot number of the line card that you want display the LEDs for.

Defaults

There are no defaults.

Command Modes

User EXEC

Command History

Release	Modification
11.2(09)GS	This command was introduced.

Usage Guidelines

This command displays the status of the line card LEDs and is useful if you are performing remote configuration or troubleshooting of a router.

Examples

In the following example, the LED status of all line cards is displayed:

```
Router# show led
SLOT 1  : RUN IOS
SLOT 6  : DNLD FABL
SLOT 7  : RP ACTV
SLOT 10 : RUN IOS
SLOT 11 : RUN IOS
SLOT 13 : RUN IOS
SLOT 14 : RUN IOS
```

The most common types of output that you see from this command and their meanings are described in the tables below.

Note If you have changed the displayed LED message using the **set card-message** command, it will be different than that specified here. These are default values only.

Note It is possible for the value of the LED to be reversed. For example, IOS RUN may be displayed as RUN IOS.

Route Processor (RP) LED Status	Description
RP UP	RP is running Cisco IOS software and functioning correctly.
MSTR RP	RP is acting as the primary RP.
SLAV RP	RP is acting as the slave RP.
RP ACTV	RP is acting as the primary RP.
RP SEC	RP is acting as the slave RP.
MEM INIT	RP is trying to size the memory.

Line Card LED Status	Description
DIAG DNLD	Line card is downloading field diagnostic software.
DIAG FAIL	Line card has failed field diagnostic test.
DIAG PASS	Line card has passed field diagnostic test.
DIAG TEST	Line card is executing field diagnostic software.
FABL DNLD	Line card is launching Fabric Downloader.
FABL WAIT	Line card is waiting to load Fabric Downloader.
IN RSET	Line card is resetting.
IOS DNLD	Line card is downloading Cisco IOS software through the switch fabric.
IOS RUN	Line card is not enabled.
IOS UP	Line card has finished loading and is now running Cisco IOS software.
MBUS DNLD	Line card is downloading Maintenance Bus (MBus) agent.
MEM INIT	Line card is trying to size memory.
PWR OFF	Line card is powered off.

If the line card status is anything other than "IOS RUN", or the RP is neither the active Master/Primary nor the Slave/Secondary, there is a problem and the card has not fully loaded correctly.

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card.
set card-message	Specifies the message that is displayed on the LED on the front panel of one or more line cards.

APPENDIX A

Glossary

active RP—The RP that controls the system, runs the routing protocols, and presents the system management interface.

APS—Automatic Protection Switching. SONET switching mechanism that routes traffic from working lines to protect them in case of a line card failure or fiber cut.

ARP—Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address.

ARPANET—Advanced Research Projects Agency Network. In 1969, the United States Department of Defense commissioned ARPANET to research networking, and the Internet revolution was born. The evolution of ARPANET into the Internet required new technologies and techniques, such as TCP/IP, Domain Name System (DNS), IP routing protocols, and the World Wide Web. The delivery of these new technologies and services allowed the ARPANET to grow into the Internet we know today as a vital part of the global economy.

ATM—Asynchronous Transfer Mode

BGP—Border Gateway Protocol. An interdomain routing protocol designed for the global Internet. Exterior border gateway protocols (EBGPs) communicate among different autonomous systems. Interior border gateway protocols (IBGPs) communicate among routers within a single autonomous system.

Cisco Express Forwarding (CEF)—An advanced Layer 3 switching technology for IP. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as those associated with the Internet, Web-based applications, and interactive sessions.

CGM—Cisco GSR Manager. An element management system for managing Cisco 12000 Series Internet Routers.

CLI—command-line interface

CSC/SFC—Clock Scheduler Card and Switch Fabric Card

Cutover—See switchover.

dCEF—Distributed CEF

DLCI—Data Link Connection Identifier. Value that specifies a PVC or SVC in a Frame Relay network.

DPT—Dynamic Packet Transfer. A resilient packet ring technology designed to deliver scalable Internet service, reliable IP-aware optical transport, and simplified network operations. Principally for metropolitan area applications, DPT-based solutions allow service providers to cost-effectively scale and distribute their Internet and IP services across a reliable optical packet ring infrastructure. DPT is based on Spatial Reuse Protocol (SRP), a Cisco-developed MAC-layer protocol for ring-based packet internetworking.

DRAM—Dynamic Random-Access Memory

EBGP—Exterior Border Gateway Protocol. EBGPs communicate among different network domains.

EHSA—Enhanced High System Availability. Redundancy method wherein the standby RP suspends its initialization midway through the startup process. See also RPR.

FIB—Forwarding Information Base. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table and is maintained by the router.

FRU—Field Replaceable Unit

FSU—Fast Software Upgrade. A mechanism to upgrade the Cisco IOS software images on the RPs and line cards without reinitializating the entire system.

Gigabit Route Processor (GRP)—Serves as the console for the Cisco 12000 Series Internet Router, handles environmental monitoring for the entire system, and provides the line cards with routing table updates.

GRP—Gigabit Route Processor

GSR—Gigabit Switch Router. Also known as Cisco 12000 Series Internet Router.

HA—High Availability

HDLC—High-Level Data Link Control

Hot swap—The feature formerly known as OIR.

HSU—Hitless Software Upgrade. Provides continued service for planned upgrade situations.

IGP—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

LANE—LAN Emulation

LC—Line card

LCP—Link Control Protocol. PPP provides LCP to establish, configure, and test the data link connection. This makes PPP more versatile, allowing it to be portable to a wide variety of environments. PPP uses LCP to automatically agree upon encapsulation format options, handle varying limits on packet size, detect a looped-back link or other common misconfiguration errors, and terminate the link. Other optional facilities provided authenticate the identity of the peer on the link, and determine when a link is functioning properly and when it is failing.

Line cards—Provide connection between the router and the network and are available in a variety of network media types (based on your order). Line cards communicate with each other and with the GRP through the switch fabric.

Mbus—Maintenance Bus

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

NetFlow—NetFlow technology efficiently provides the metering base for a key set of applications including network traffic accounting, usage-based network billing, network planning, network monitoring, outbound marketing, and data mining capabilities for both service provider and enterprise customers. Cisco provides a set of NetFlow applications to collect NetFlow export data, perform data volume reduction and post-processing, and provide end-user applications with easy access to NetFlow data. Cisco is currently working with a number of partners to provide customers with comprehensive solutions for NetFlow-based billing, planning, and monitoring. NetFlow also provides the measurement base for Cisco's Internet Quality of Service (QoS) initiatives. NetFlow captures the traffic classification or precedence associated with each flow, enabling differentiated charging based on Quality of Service.

NSF—Non-Stop Forwarding. The ability of a router to continue to forward traffic toward a router that may be recovering from a transient failure. Also, the ability of a router recovering from a transient failure in the control plane to continue correctly forwarding traffic sent to it by a peer.

NVRAM—Non-volatile RAM

OIR—Online Insertion and Removal. Feature that permits the addition, replacement, or removal of cards without interrupting the system power, entering console commands, or causing other software or interfaces to shut down. Also called "hot swapping" or "power-on servicing".

OSPF—Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.

PCMCIA—Personal Computer Memory Card International Association. PCMCIA is an organization that developed a standard for small, credit card-sized devices, some of which are used as Flash memory disks in Cisco routers.

PIM—Protocol Independent Multicast

POS—Packet-over-SONET interface. Enables core routers to send native IP packets directly over SONET/SDH frames.

Primary RP—Term previously used for active RP.

PRP—Performance Route Processor

PSAR—Packet Segmentation and Reassembly

PVC—Permanent Virtual Circuit

RAM—Random-Access Memory

RIP—Routing Internet Protocol. IGP supplied with UNIX BSD systems. The most common IGP in the Internet. RIP uses hop count as a routing metric.

ROM—Read-Only Memory

RP—Route Processor

RPF—Return Path Forwarding

RPR—Resilient Packet Ring. See DPT.

RPR—Route Processor Redundancy. In RPR, line cards are reset on switchover and line card software is reloaded.

RPR+—Route Processor Redundancy Plus. An enhancement to RPR/EHSA in which the standby RP is fully initialized. An RPR+ switchover does not involve line card reset or line card software reload.

RSVP—Resource Reservation Protocol. RSVP is a network-control protocol that enables Internet applications to obtain special qualities of service (QoSs) for their data flows.

Secondary RP—Term previously used for standby RP

SIMM—Single Inline Memory Module

SNMP—Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SSO—Stateful switchover. SSO provides protection for network edge devices with redundant processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

standby RP—The RP that waits in case the active or primary RP fails.

SVC—Switched Virtual Circuit

Switch fabric—The circuitry that carries the user traffic between line cards or between the GRP and a line card.

Switchover—An event in which system control and routing protocol execution is transferred from a failed processor to a standby RP.

VC—Virtual Circuit. Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC).

VCI—Virtual Circuit Identifier.

VLAN— Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VOFR—Voice over Frame Relay. Voice over Frame Relay enables a router to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. When sending voice traffic over Frame Relay, the voice traffic is segmented and encapsulated for transit across the Frame Relay network using FRF.12 encapsulation.

VPI—Virtual Path Identifier.

VPN—Virtual Private Network. VPNs are networks deployed on a public network infrastructure that employ the same security, management, and quality of service policies applied in a private network. Benefits of using VPNs include cost savings and extending connectivity to telecommuters, mobile users, and remote offices, as well as to new constituencies, such as customers, suppliers, and partners.

VRF—Virtual Route Forwarding

INDEX